

LIFARS

your digital world, **secured**

NYCFE Fraud Conference

www.lifars.com



Agenda

LIFARS
your digital world, secured

3	About Me
4	Fraud vs. Misrepresentation Introduction
5-6	Fraud vs. Misrepresentation Case Study
7-8	Fraud vs. Misrepresentation
9	Fraud vs. Cybercrime
10	What Happens Where there is Fraud and Computer Crime
11	Misrepresentation of Computer Crime vs. Fraud
12	Internal Systems Controls
13	Risk Mitigation Strategies
14	Risk Types
15-16	Cybersecurity Maturity Level
17	Fraud and Computer Crime
18	Digital Forensics
19	About LIFARS
20	Questions

© 2021 LIFARS, LLC All Rights Reserved.

About Me

LIFARS
your digital world, **secured**



Dr. Ondrej Krehel
Digital Forensics Lead,
CEO and Founder, LIFARS LLC

I have conducted a wide range of expert witness testimonies, red team exercises, cyber resilience matters, investigations, including data breached through computer intrusions, theft of intellectual property, massive deletions, defragmentation, advanced file recovery and carvings, anti-money laundering, financial fraud, mathematical modeling and computer hacking.

- Actively participate in high-profile engagements around the globe
- Created a proprietary methodology to achieve the most rapid root-cause analysis and remediation.
- Former lecturer at FBI Training Academy
- Former Chief Information Security Officer of IDT911
- Led forensic investigations and cybersecurity consulting at Stroz Friedberg

Frequent speaker at industry events and author on matters related to information security and computer forensics. My work has received attention from CNN, ABC, BBC, Reuters, Bloomberg, The Wall Street Journal and The New York Times.

Education:

- Ph.D. in Computer Forensics from Police Academy in Bratislava
- M.S. degree in Mathematical Physics from Comenius University
- Engineering Diploma from Technical University in Zvolen, Slovakia

© 2021 LIFARS, LLC All Rights Reserved.

LIFARS
your digital world, secured

Introduction

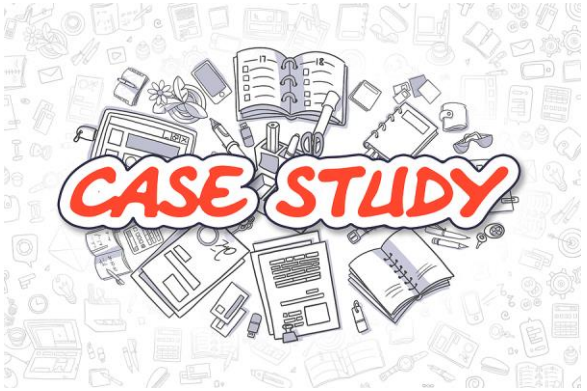
This cyber insurance claims and compliance session will explore cyber insurance claims from the point of view of potential fraud issues that can arise related to internal audit statements, insurance coverage remediation challenges, digital forensic analysis, privacy coverages, identity protection, and the involvement of internal and external legal counsel.

We will walk through real-world examples and review the challenges faced during investigations, and during claim settlement negotiation between the victim and the insurance carrier. Scenarios will include misrepresentation of internal audits statements, internal systems controls, and cybersecurity maturity level.

© 2021 LIFARS, LLC All Rights Reserved.

Case Study

LIFARS
your digital world, secured



Affinity filed a breach report with the HHS Office for Civil Rights (OCR) on April 15, 2010, as required by the Health Information Technology for Economic and Clinical Health, or HITECH Act. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information.

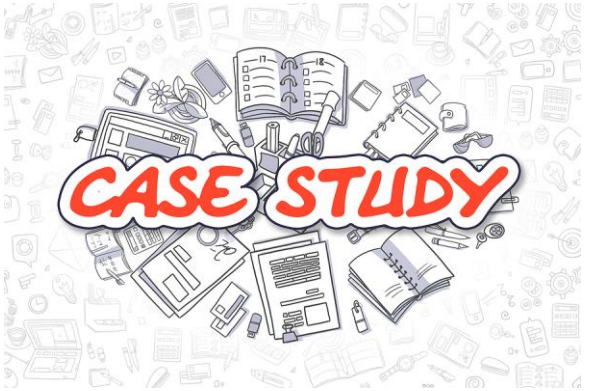
Affinity indicated that it was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive.

View Press Release

© 2021 LIFARS, LLC All Rights Reserved.

Case Study

LIFARS
your digital world, secured



Affinity estimated that up to 344,579 individuals may have been affected by this breach. OCR's investigation indicated that Affinity impermissibly disclosed the protected health information of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives.

In addition, the investigation revealed that Affinity failed to incorporate the electronic protected health information (ePHI) stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

HHS Settles with Health Plan in Photocopier Breach Case

© 2021 LIFARS, LLC All Rights Reserved.

LIFARS
your digital world, secured

Fraud (is a type of misrepresentation)

Elements to prove a claim for fraud:

- A false statement regarding a material fact
- Knew or should have known the representation was false
- Intended that the representation induce insurer to act
- Insurer suffered damages in justifiable reliance on the representation



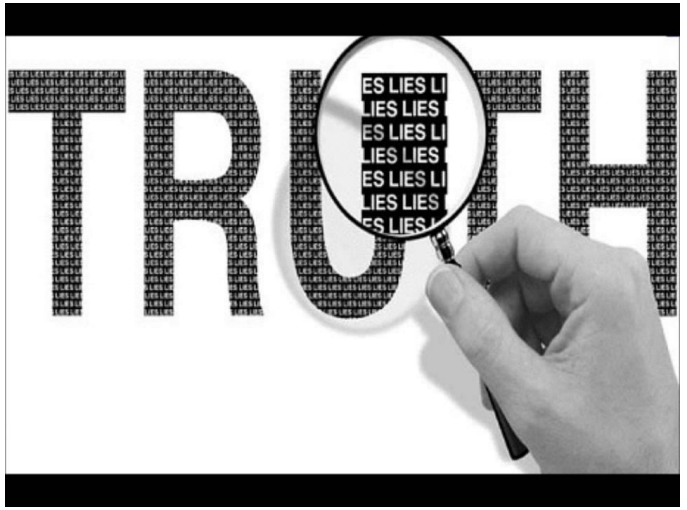
© 2021 LIFARS, LLC All Rights Reserved.

LIFARS
your digital world, secured

Misrepresentation

- Deliberate misrepresentations - when a policyholder does not disclose or if the insured misrepresents a matter which they know would influence the insurer's judgment in deciding whether to insure the risk, the policy terms.

- Careless misrepresentations - when a policyholder does not intend to deliberately mislead. This could be due to a mistake by staff or if the questions asked were not clarified.



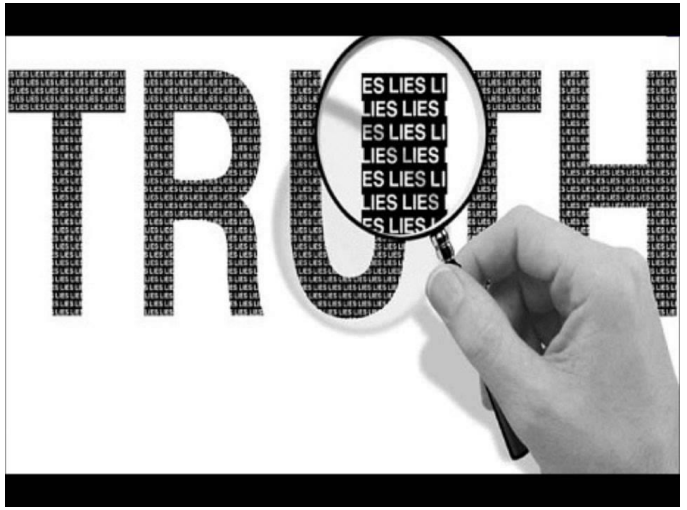
© 2021 LIFARS, LLC All Rights Reserved.

Fraud vs. Cybercrime

LIFARS
your digital world, secured

Fraud

- Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person .



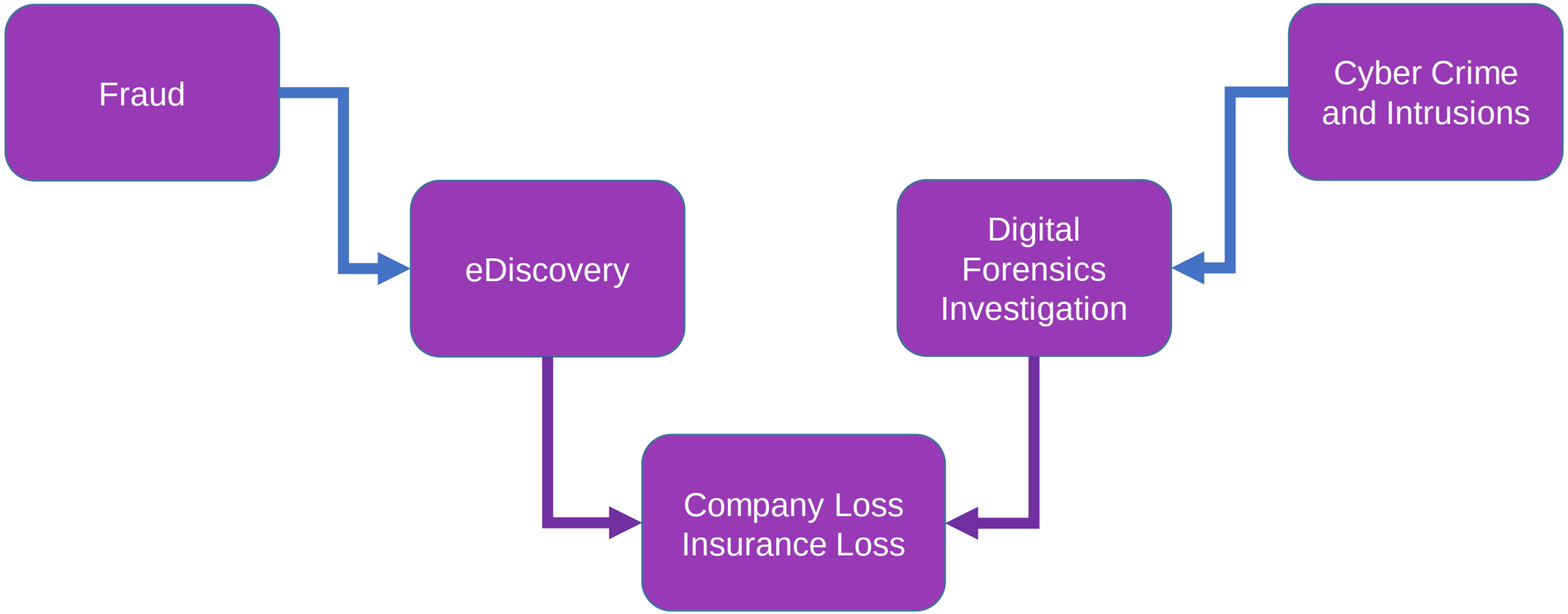
Cybercrime

- Cybercrime is any criminal act dealing with computers and networks.

© 2021 LIFARS, LLC All Rights Reserved.

What Happens Where there is Fraud and Computer Crime

LIFARS
your digital world, secured



© 2021 LIFARS, LLC All Rights Reserved.

LIFARS
your digital world, secured

ACH Case Study

- US Company leaves in African country heavy infrastructure with very powerful Internet.
- Banks in Middle east, such as Dubai, are affected from US ACH transfers
- 5 Billion devices run Java.
- ACH intermediary bank cannot find from the received batch where the issue is...
- Money mules collect money from various locations under 1 hour.
- Average loss per one ACH attack was $28,000.
- Average loss per month $420,000.
- Threat actors are modifying original data coming in, or directly manipulating received ACH instructions.
- Insiders and Fraud is a suspect.

https://lifars.com/knowledge-center/case-study-hacking-as-a-service/

© 2021 LIFARS, LLC All Rights Reserved.

LIFARS
your digital world, secured

Fraud

- Financial controls around monetary flows – example wire transfer.
- Internal audit related to computer system accuracy – such as access to database systems for reporting – intrusion can modify system.
- SEC is very slow, and 10-K Statements have limited information.
- Institutions are dealing with fraud in different ways, and reporting varies, which also dictates internal controls mapping .

Computer hacking

- Visibility into network and computer systems by monitoring and detection
- Ability to deal with incidents and events, be able to probe by threat hunting.
- Commercially reasonable practices implemented – banking and wire fraud.
- Conduct Assessments: IR Readiness Assessment, Cyber Risks, Penetration test.

© 2021 LIFARS, LLC All Rights Reserved.

Risk Mitigation Strategies

Accept: If risk is at an acceptable level, has a sufficiently low estimated failure rate, accept the risk.

Transfer: Shift the burden of the risk consequence to another party.

Mitigate: Reduce the severity of a risk, by implementing controls. Controls that detect causes of unwanted events prior to the consequence occurring, or the detection of root causes of unwanted failures that the team can avoid.

Avoid: If a risk presents an unwanted negative consequence, avoid those consequences.



© 2021 LIFARS, LLC All Rights Reserved.

Risk Types

Strategic: Decisions that an organizations' management takes about products/services. These could be risks associated with the development of products/services and risks from the technological view (cybersecurity) which impact a business.



Operational: An organization and associated third-party networks and systems are susceptible to risk of breaches. Nefarious cyber activities could lead to theft, loss, disclosure of confidential information, reputation damage, regulatory penalties, legal exposure, and financial losses. .

Compliance: When industry and Government regulations are not followed it can result in detrimental to your organization and inflict financial penalties and possible imprisonment..

© 2021 LIFARS, LLC All Rights Reserved.

Cybersecurity Maturity Level

LIFARS
your digital world, secured

ESG follows a more general approach to try and categorize the overall attitude and dedication towards security within an organization. Using this model as a bar, you can establish your organization's maturity level by assessing how closely your relationship with security matches one of the four categories.

Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and ad-hoc. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security.

Source: Enterprise Strategy Group, 2014.

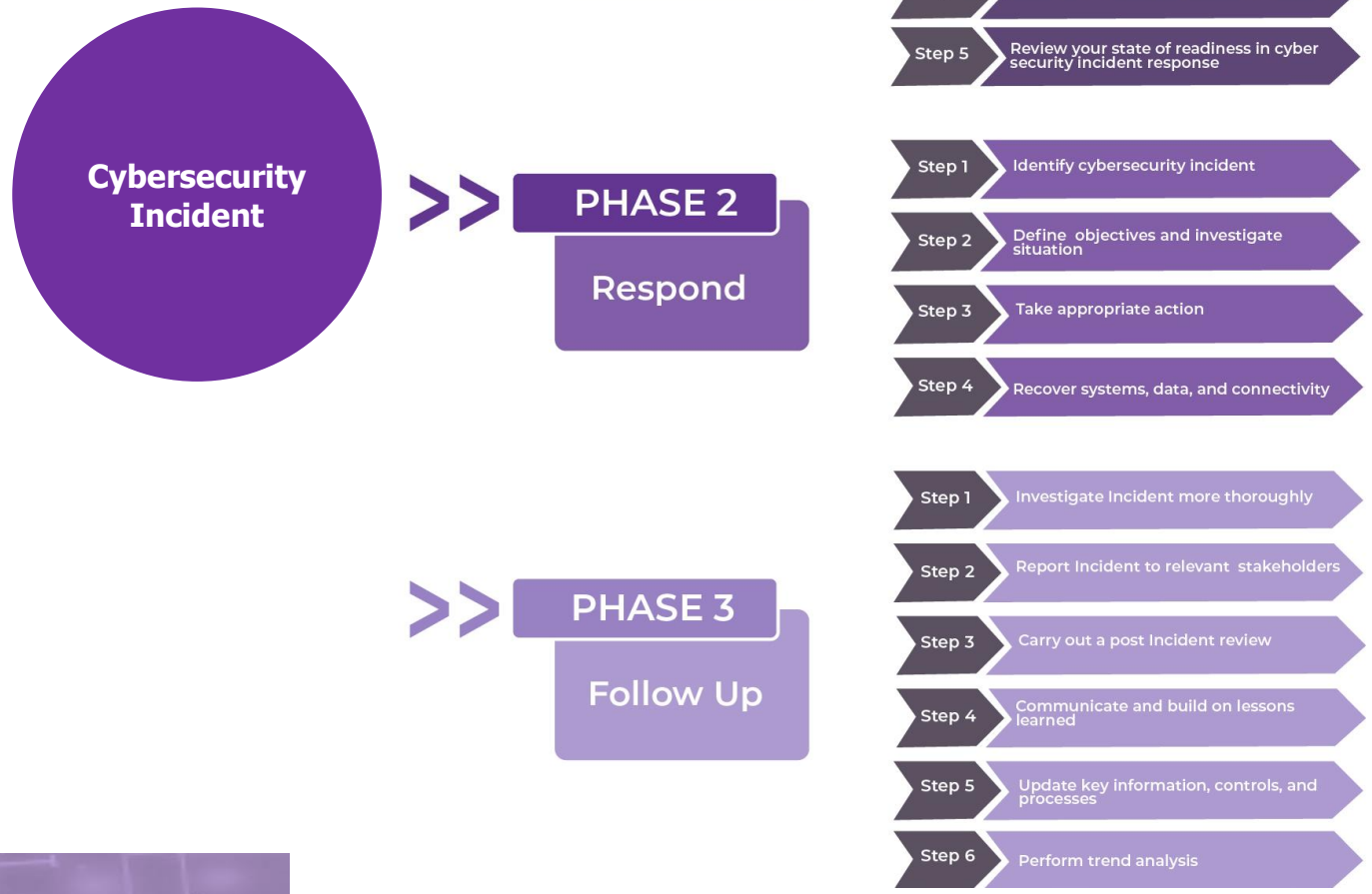
© 2021 LIFARS, LLC All Rights Reserved.

Cybersecurity Maturity Level

LIFARS
your digital world, secured

Paradigms that can help you analyze your current maturity and provide concrete steps to mature it further.

The CREST Incident Response Maturity Assessment specifically helps assess the status of an organization's cybersecurity incident response capability. It consists of 5 maturity levels: foundation, emerging, established, dynamic, and optimized. It also provides a roadmap that consists of 15 steps across 3 phases to improve your incident response maturity

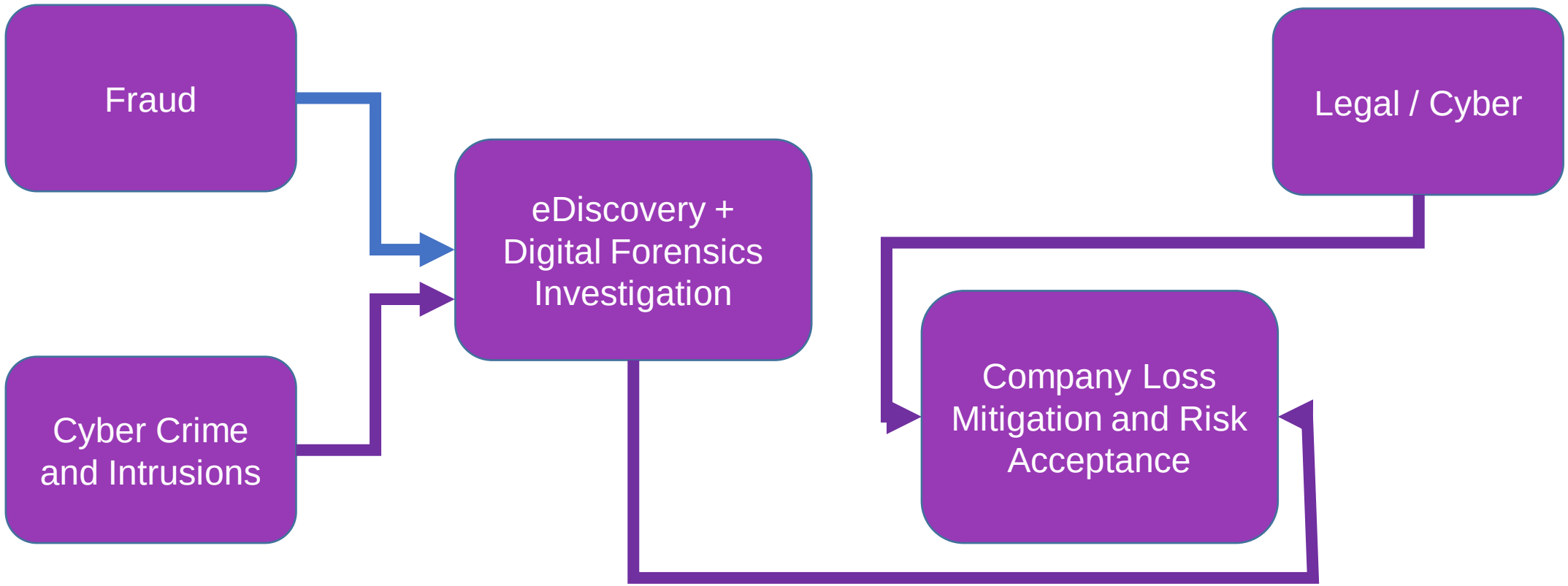


No matter which model you end up employing, they typically involve several common steps:

- Assessing your current security readiness
- Set goals in terms of your target maturity level, including timeframes and phases
- Don't view it as a set-it-and-forget-it solution but keep refining your cybersecurity through data collection, analysis, and iterative improvements

© 2021 LIFARS, LLC All Rights Reserved.

Fraud and Computer Crime



© 2021 LIFARS, LLC All Rights Reserved.

Digital Forensics

LIFARS
your digital world, secured

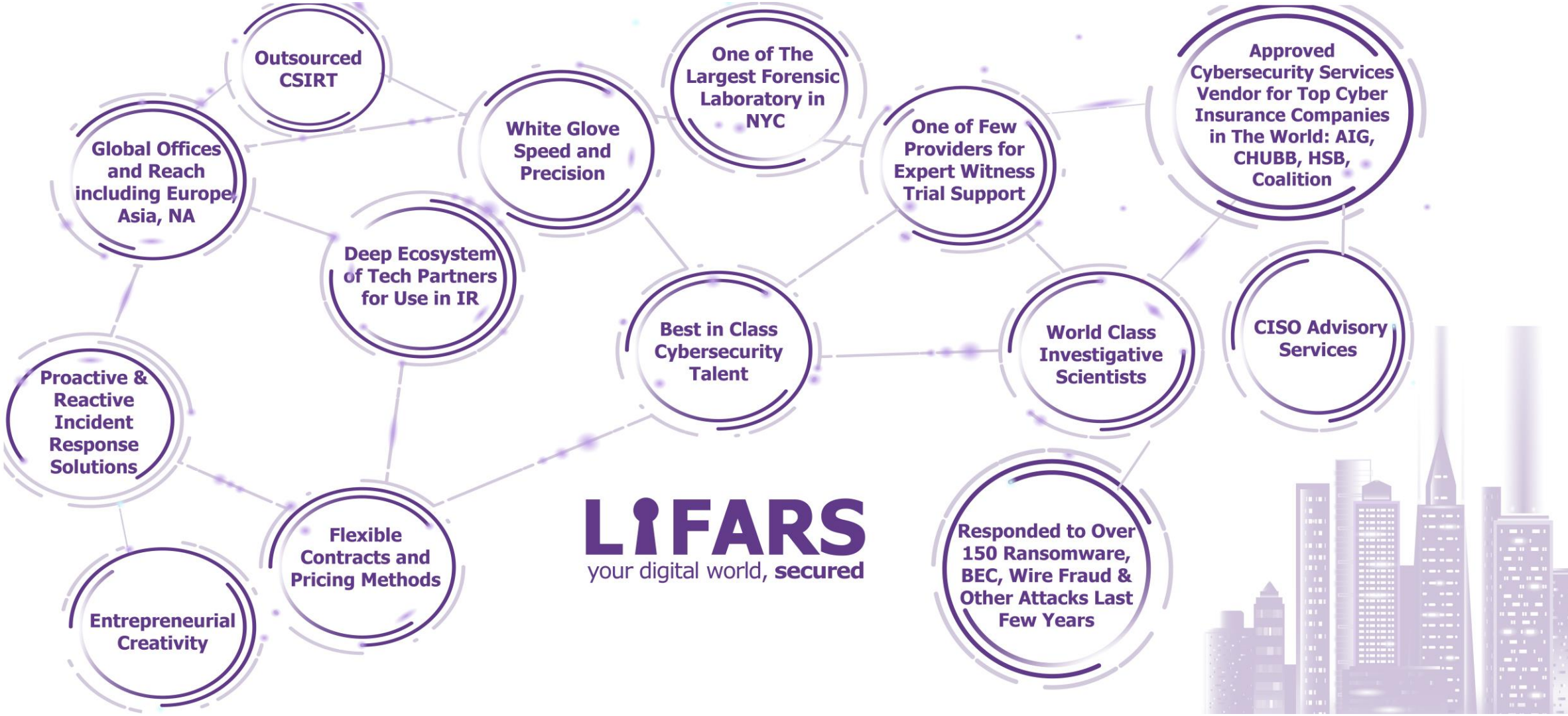
Digital forensics leverages specialized techniques and tools to investigate various forms of computer-related crimes. Digital crimes may include network intrusion, and illicit use. The aim of digital forensics is to present evidence exactly as it is on the system, in a way that can be replicated by following the exact steps. Digital forensics comes in all shapes and sizes, with different examination methods for each. The areas below give a glance to some of the main divisions:

- **Computer forensics** – Analysis of information contained within and created with computer systems and computing devices.
- **Mobile device forensics** – Analysis of cellular phones, smart phones and MP3 players.
- **Network forensics** – Analysis and monitoring of traffic on computer networks ranging from LANs to WANs and the Internet.
- **Database forensics** – Analysis of databases, including metadata, for incidents such as security attacks.

Collection and analysis help provide court-admissible evidence and aid law enforcement in court proceedings. Our Digital Forensics team provides expert witness testimony.

© 2021 LIFARS, LLC All Rights Reserved.

LIFARS



© 2021 LIFARS, LLC All Rights Reserved.

LIFARS
your digital world, **secured**

THANK YOU

LIFARS

your digital world, **secured**

QUESTIONS

?

contact@lifars.com 212-222-7061 www.LIFARS.com

© 2021 LIFARS, LLC All Rights Reserved.