Design of a Framework for the Best Practices in Computer Forensics within the Cybersecurity Infrastructure in the Regulated Industry

Eduardo Vázquez Ruiz
Master in Computer Science
Advisor: Jeffrey Duffany, Ph.D.
Electrical and Computer Engineering & Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— We cannot ignore the fact that hackers have been evolving and growing to the level that there are more hackers with the attraction to do evil than Ethical Hackers. Cyber-attacks are a growing threat for companies, and these do not discriminate the size of industry or the sector to which it belongs, so in reality no company or person is immune to an attack of this type. This article is focused directly on the design of a Framework based on the join of the most important systems Cybersecurity and Forensic Analysis to avoid attacks in regulated industries and if we were already attacked, we know how to solve them. As we can see later in section 2, the technology has been evolved in an advanced way in the last ten years and along with this, there is the evolution of cyber-attacks. During this Article we will be able to appraise the important concepts within the good practices in the industry and see an incorporation of these in a Framework that unites the cyber-industry and the Forensic analysis, so that the use of this format can facilitate the industry incorporate their methodologies without them being affected.*

Key Terms *— Cybercrime, Digital Evidence, Digital Investigations, Framework.*

INTRODUCTION

When we talk about Computer Forensics we can understand that it is related to an event that occurred or a crime committed where a device or computer system is involved. The field of computer forensics is one of the newer disciplines in forensic science. Like all the others, it is going through a transition from an art practiced by individuals to a more standardized set of techniques for which “best practices” can be defined. But what happens if this is entirely related to a regulated industry company? We know there are some differences between what Cybersecurity and Computer Forensics is, but when we see it closely we know their relationship. In this article we're just going to reviews the existing methodologies and best practices for digital investigations phases in a regulated environment.

Computer Forensics

Computer forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. More recently, Regulated Industries have used computer forensics to their benefit in such a variety of cases:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Forgeries
- Bankruptcy investigations
- Inappropriate email/internet use in the work place
- Regulatory compliance

Cybersecurity

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises cybersecurity and physical security both are used by enterprises to protect against unauthorized access to data centers and other computerized systems.

Ensuring cybersecurity requires the coordination of efforts throughout an information system, which includes:

- Application security
- Information security
- Network security

- Disaster recovery/business continuity planning
- Operational security
- End-user education

Regulated Industry and Cybertechnology: The Need for Best Practices

According to Cisco [1], in 2020 the number of devices connected to the Internet will exceed 50 billion, but as the number of devices connected to the Internet grows, so does the number of threats. Therefore, not only the industry will benefit from this new revolution, but, unfortunately, cybercriminals will also do it through the perpetration of attacks, whether through the payment of ransoms, extortion or the sale of information in the Deep Web.

Several approaches can be identified according to the objectives and needs to which they respond, among which the following can be mentioned:

- Related to personnel policies
- Performance
- Organizational culture

What benefits can best practices bring in a company?

- It is easier to build a strong and favorable work culture.
- Priorities are recognized, and processes are efficient.
- Increase organizational flexibility.
- Professional recognition grows.
- Leadership is promoted.
- Better operational and economic results are obtained.

Applying best practices can mean great benefits for companies and work groups, so in addition to knowing them, it is advisable to analyze them to consider their possible implementation in the professional space.

IT Role in the Regulated Industry and the Fundamental Principles

In IT Security field, there are a lot of technological aspects, such as access control, biometrics, encryption, network security, security algorithm, etc. Each of them has its specific methodology, but they all rely on one set of fundamental principles. That is, the core IT Security fundamentals Confidentiality, Integrity and Availability (figure 1). This fundament comes from the ISO 27000 standards. ISO 27000 is a series of standards and related terms that provide guidance on matters of information security.

Figure 1
Fundamental Principle in Information Security [2]

With this core principle, different areas of IT Security are linked together. In the same way that we see these links we can understand that the regulated industry needs a growth in terms of cybersecurity is concerned since the dependence of different systems in the industry are depending on high technology.

The Industrial Control Systems (ICS)

Industrial Control Systems (ICS) are used worldwide in critical infrastructures. The term "critical infrastructure" conjures up images of highways, electrical grids, pipelines, government facilities and utilities. The Department of Homeland Security defines critical infrastructure as "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters".

Statistics

Although awareness and investment have increased, companies continue to be victims of

more conventional threats. Typical examples are malware and ransomware. As per the report [3]:

- 64% of industrial companies experienced at least one attack of conventional malware or viruses.
- 30% suffered a ransomware attack.
- 27% suffered a breach in their ICS due to errors and reckless actions of employees.

Workers are the weakest link in the chain and the easiest objective for cybercriminals to access the industrial network. Targeted attacks represented only 16% in 2018 (compared to 36% in 2017).

Cost of Cybercrime

In spite of the gaps in data and the reliability issues noted above, recent works by Dreyer [4], Riek et al. [5] and Romanosky [6], among others, provide measurement tools and models for estimating cybercrime costs and represent continued in-roads into the systematic accounting of costs. There are five types of costs [7]:

- Criminal revenue, the monetary equivalent of the gross receipts from a crime
- Direct losses, the monetary equivalent of losses, damage, or other suffering felt by the victim because of a cybercrime
- Indirect losses, the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, no matter whether successful or not and independent of a specific instance of that cybercrime
- Defense costs, the monetary equivalent of prevention efforts
- Costs to society, the sum of direct losses, indirect losses, and defense costs

FRAMEWORK DESIGN

The Design of this Framework takes as reference the NIST Cybersecurity Framework [8]. The NIST Cybersecurity Framework (figure 2) provides a policy framework of computer security guidance for how private sector organizations that's include the Regulatory Industries in the United States can assess and improve their ability to prevent, detect, and respond to cyber-attacks.

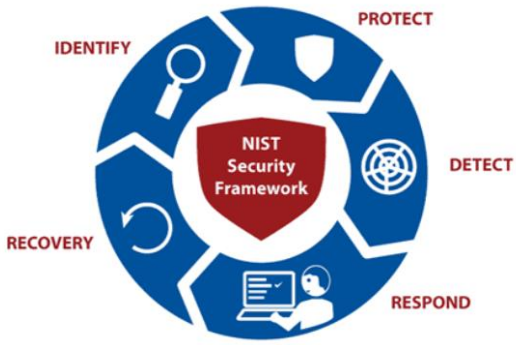


Figure 2
NIST Cyber Security Framework [8]

Binding Them All

In a typical digital forensics investigation process for a regulated Industry, system owners, IT investigators (digital forensics) and legal practitioners are expected to be involved. However, if we further separate the roles and responsibilities of these participants, they could be further categorized into eight individual roles of participants in investigation. These roles are different in nature but could be handled by the same person if required [9].

- Case leader: The planner of the entire digital investigation process.
- System/business owner: The owner of the system being inspected. He/she is usually the victim and sponsor of the case.
- Legal advisor: The first legal practitioner the case leader would seek for legal advice.
- Security/system architect/auditor: Should be interviewed.
- Digital forensics specialist: Plans the entire operations.
- Digital forensics investigator/system administrator/operator
- Digital forensics analyst
- Legal prosecutor

PRESENTING THE DESIGN

A Regulated Industry can use the Framework as a key part of its systematic process for

identifying, assessing, and managing cybersecurity risk. Figure 3 shows the design of the Framework proposed for a regulated industry.

The regulated Industry has his own gestion system and his process as the Quality compliance and the manufacturing process and procedures. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

Framework Analysis in a Basic Work Environment

Table 1 shows the framework core that should be used and the different places (in the subcategory column) where the assets should be placed in their categories. These are Identify, Protect, Detect, Respond and Recover. Where we can see that the answer shows how you should respond in case of an attack or event.

The following Phases in steps illustrate how an industry could use the Framework Core shows in table 1 to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity and analysis forensics. The same Framework in Phase 2 takes you directly to the resolution of the problem found in the case of having one [10].

Phase 1: Improving Cybersecurity

- **Step 1:** Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities.
- **Step 2:** Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

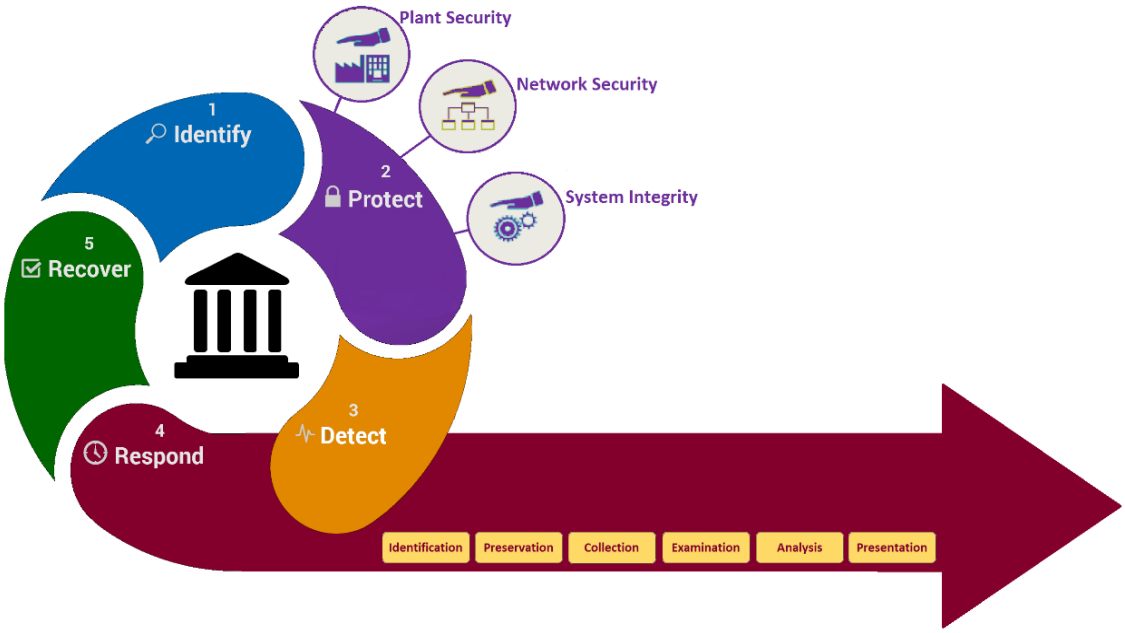
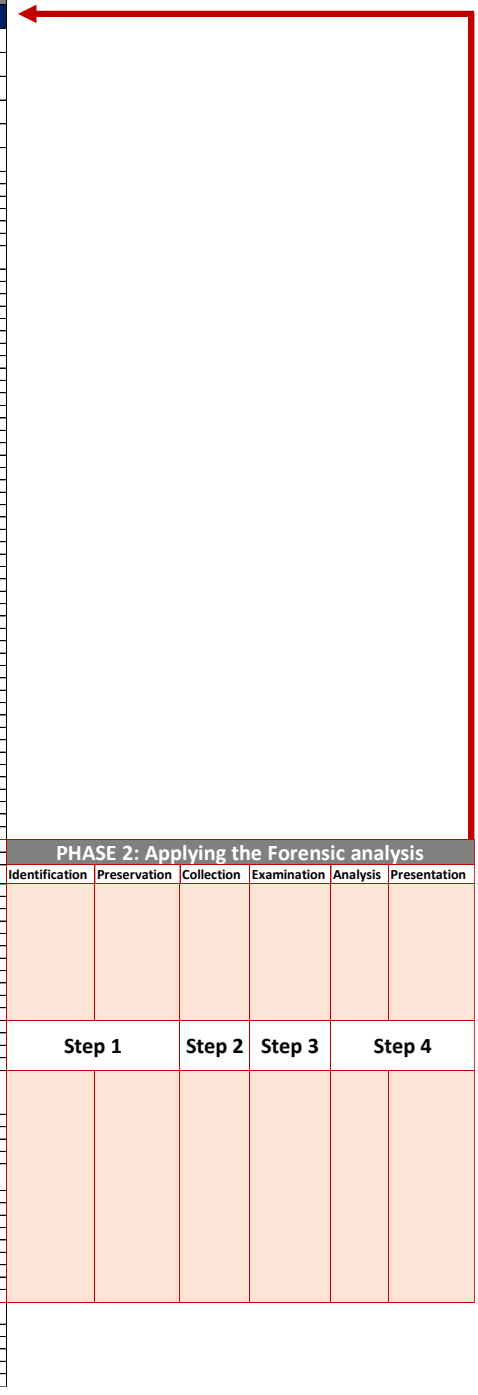


Figure 3
Framework Design for a Regulated Industry

Table 1

Framework Core Process Model

PHASE : Improving Cybersecurity		
Function	**Category**	**Subcategory**
IDENTIFY (ID)	Asset Management	
	Business Environment	
	Governance	
	Risk Assessment	
	Risk Management Strategy	
PROTECT (PR)	Access Control	
	Awareness and Training	
	Data Security	
	Information Protection Processes and Procedures	
	Maintenance	
	Protective Technology.	
DETECT (DE)	Anomalies and Events	
	Security Continuous Monitoring	
	Detection Processes	
RESPOND (RS)	Response Planning (RS.RP)	
	Communications	
	Analysis	
	Mitigation	
	Improvements	
RECOVER (RC)	Recovery Planning	
	Improvements	
	Communications	



- **Step 3:** Create a current profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.
- **Step 4:** Conduct a risk assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities
- **Step 5:** Create a target profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes.
- **Step 6:** Determine, analyze, and prioritize gaps. The organization compares the Current Profile and the Target Profile to determine gaps.
- **Step 7:** Implement action plan. The organization determines which actions to take on gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile.

Phase 2: Applying the Forensic Analysis Inside the Framework if the Case is Detected

- **Step 1:** Study of the initial situation. An Analysis of the scenario will be carried out and a copy or replica of the data sources will be constructed. In this phase, there will also be a planning of the tests.
- **Step 2:** Startup of the evidence for the evidence analysis. Any trace that can be detected is analyzed: volatile memory, existing files, password protected files, hidden files, various records of the system, etc.
- **Step 3:** Diagnosis of the scenario. In this phase the results of the tests carried out are detailed and reports are written on the information systems that have been affected, identification of the author, methods used, and weaknesses attacked. Subsequently, a definition of the corrective actions will be detailed, the vulnerabilities identified.
- **Step 4:** Implementation of the corrective actions. These corrective actions will be applied to improve the security measures of the company. In this respect, the Loop is applied again for continuous improvement. An organization may repeat the steps as needed to continually assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments.
- **Step 5:** Present the case for possible eventualities.

These corrective actions will be applied to improve the security measures of the company. In this respect, the Loop is applied again for continuous improvement. The organization may repeat the steps as needed to continually assess and improve its cybersecurity.

Testing the Framework

To verify the efficiency and operation of this Framework, it was put into practice in a normal regulated environment and it was decided to compare the current status with the new one, in this case a regulated company was chosen as an example to analyze this scenario. As we can know due to the amplitude and scope of the regulated environment of this company and the many areas that occupy it, different security frameworks are composed. In this case we will focus only on a specific area since an analysis of the Framework for the whole industry would entail months of adaptation because it has its regulations not only in cyber security but also in areas of compliance. In this environment, levels of cybersecurity are basic, closely related to those we know.

It is important that we know that this analysis is done in a test environment; many of the steps that we already know within the IT margin are going to be ignored and many of the documentation required for this Framework will be assumed as Completed.

This Framework assembles and organizes the Company standards, guidelines, and practices that are working effectively. This Framework is user-

friendly and is intended for use by the leaders and managers in the organization who are concerned with and responsible for mission-driven, cybersecurity-related policy and operations. See section “IT role in the Regulated Industry”. These leaders and managers may include senior leaders, chief security officers, and chief information officers, among others. For these and other roles and functions, and the benefits to each of using the Framework, see the section “The Typical IT Infrastructure.” For this test it was only possible to obtain approval of the manufacturing offices area.

Because cybersecurity is an organization-wide concern, before of start to organize the Framework, this must be including questions about:

- your organizational and your cybersecurity leaders,
- cybersecurity in the context of your organization’s overall strategy,
- the cybersecurity needs and expectations of internal and external customers,
- the measurement of cybersecurity performance in the context of overall performance measurement,
- your overall workforce and your cybersecurity workforce,
- your overall and your cybersecurity suppliers and partners,
- your cybersecurity operations and their alignment with overall operations, and
- results related to each of these areas.

With this question this framework will leads us to understand the organization’s cybersecurity policies and operations in the context of its unique characteristics, strategic situation, and cybersecurity risks.

Organizational Context

The Organizational Context is a snapshot of the organization and its strategic environment. With a clear understanding of the organization.

In our case, in order not to extend the analysis, a number of documents must be analyzed and delivered to the directors or Supervisor in Charge for structuring the Framework. It is important to mention that most of the essential documents are provided by the industry for the organization of these within the framework.

Current Environment

In this case the company basically use similar general steps required for incident identification, detection, and analysis based in the good practiced, this step is to:

- A review Internal Audit guideline for department personnel actions with regard to unacceptable computer use and other cyber security incidents.
- To determine whether an incident has occurred.

Coordination between the IT Security Office and the affected department is important to make sure that steps taken to verify the incident do not alter data that will be needed for further investigation.

A coordinated investigation may be required once an incident has been confirmed. The IT Security Office will identify and assign an individual to be the Incident Response Manager (IRM).

All personnel may be alerted to a threat from an internal or external source. In the case a threat has been detected the assigned person must be to notify IT Security Office once.

- The local systems administrator is responsible for fixing the problem on the machine(s) The IT Security Office may also detect a threat and alert the system custodian of record for the hardware or Ethernet port connection.
- All incidents should be handled by departmental IT staff with the support of the IT Security Office.

It is important to emphasize that this industry in the way of working forensic cases are not related to a specific framework and these are worked through a line related to the case that is occurring.

Testing with a Software

The use of software is very favorable in these cases for the handling of documents according to the category assigned within the Framework.

Types of software which are very favorable to use and adapt the framework are those focused on the creation of databases. As for example Access, MySQL, QLServe, FoxPro and even Oracle itself.

In our case, NIST (National Institute of Standard and Technology) provides a part of a software based on File Maker that we can analyze using our frame of reference since it is intertwined or related to the cybersecurity framework of NIST.

The software used is NIST_CSF_Tool_1.0-WIN. This software is created by NIST in File Maker Pro and we can use it for the editing of our framework. The analysis of this would facilitate the inclusion of the different documents of the industry in a referential frame.

Analyzing the Software

The software uses the database as a starting point and this gives us the ability to navigate from the beginning with the chain of elements (figure 4). As you incorporate the elements you can navigate through them.

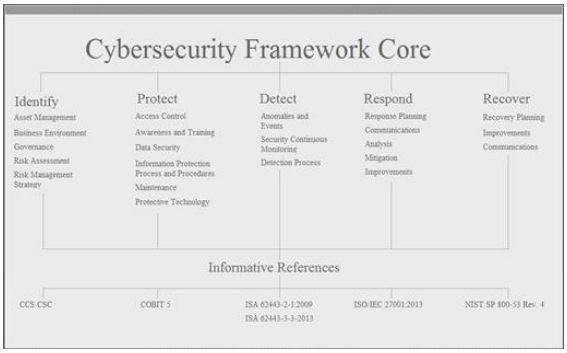


Figure 4
Home Screen

The Framework provides the required program elements.

Identify and Protect

In this area we will place the documentation related to our Framework (figure 5). It is important to consider all the regulations within the framework, even if they are not directly related to cybersecurity as long as the Framework can be completely aligned to the Industry.

Figure 5
Identify and Protect Software Screen

Detect and Respond

In the case to this project, a forensic threat would not be allowed for proves because of the regulation the industry, but we can signal that the preparation of identifiers was initialization in our test, that are: identification, preservation, collection, examination, analysis, presentation (recover) (figure 6).

In this case as mentioned above we can add it as part of our software if we use a more personalized one, as we can also use our Framework Core Table (table 1) which is what we will do after obtaining the software summary.

Figure 6
Detect and Respond Software Screen

Recover

As we indicated earlier, this scenario is always shown if we carry a threat, or a vulnerability detected, otherwise this Framework gives us the ability to maintain the continuous improvement as provided by the cycle of best practices.

Incorporating the Data and Documenting in the Framework

Selecting each one of the elements this directs us to the data base for each element (figure 7). This is where reports and documents are incorporated.

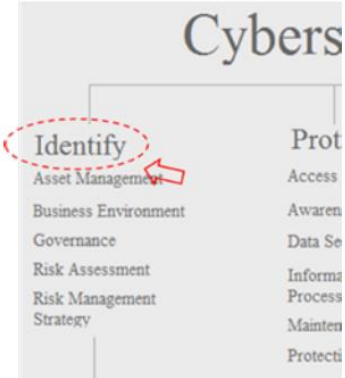


Figure 7
Selecting Example

At the bottom of the Menu this shows us the area of informative documents for this ISO regulated industry and the quality and compliance documents can be incorporated as this can relate us to cybersecurity (figure 8).

Figure 8
Informative Reference Software Screen

After entering all the information obtained, this will save how the information is recorded in the database using Excel (figure 9).

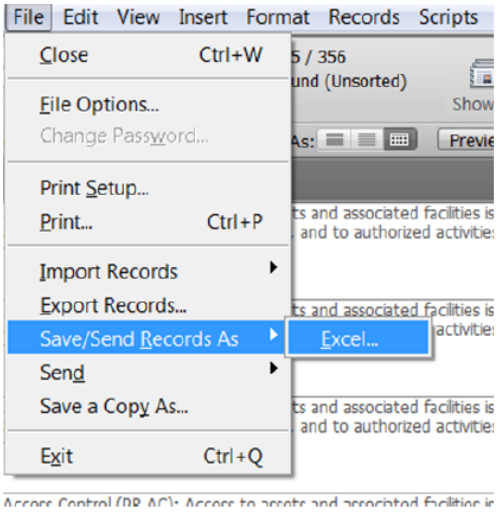


Figure 9
Save/Send Records Example Screen

This will generate a table in excel with most of the framework addressed. Now is the time when we can complete our Framework by completing the Forensic Analysis action and directing the information to this section (table 2).

Table 2
Zoom of the Forensic Area in Table 1

			PHASE 2: Applying the Forensic analysis					
			Identification	Preservation	Collection	Examination	Analysis	Presentation
DETECT (DE)	Anomalies and Events							
	Security Continuous Monitoring							
	Detection Processes		Step 1		Step 2	Step 3	Step 4	
RESPOND (RS)	Response Planning (RS.RP)							
	Communications							
	Analysis							
	Mitigation							
	Improvements							

This more organized way shows us that it is easy to detect any vulnerability at any point that is not being monitored. The continuous way of carrying the Framework will facilitate the long-term improvement due to changes in technology.

CONCLUSION

In order to understand and justify this Framework and what we see in the Industry's regular behavior, we can divide its strengths thus:

- **Abnormalities and events:** This supports the first stage of our framework. The anomalous activity is detected in a timely manner and the potential impact of the events is understood. The most important terms in this brief definition are detect and understand. Obviously, the first key is to detect the event in a timely manner. What is a timely manner?
- **Continuous security monitoring:** Threats change every day and the methods that hackers use to access their systems change every day.
- **Detection processes:** In the regulated industry, processes and procedures are very important. Having a process or processes and procedures is great; however, if you have processes and procedures in place, but do not test or practice them, hackers are being given an advantage.

The choice to use a particular IT security framework can be driven by multiple factors. The type of industry or compliance requirements could be deciding factors. The ISO 27000 series that is used for the Industry is the magnum opus of information security frameworks with applicability in any industry, although the implementation process is long and involved. However, it is best used where the company needs to market information security capabilities through the ISO 27000 certification, and this is the case. This proposed Framework in this article also can be used by any company and not necessarily a regulated industry to build a technology-specific information security plan. Any of them will help a security professional organize and manage an information security program. The only bad choice among these frameworks is not choosing any of them.

REFERENCES

[1] D. Evans. (2011, April). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," in *Cisco IBSG, San Jose* [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[2] M. M. Weiss, "Compliance Law Requirements and Business Drivers," in *Auditing IT Infrastructures for Compliance*, 1st ed. Ontario: World Headquarters, 2011, ch. 8, sec. 2, pp. 169–188.

[3] W. Schwab and M. Poujol. (2018, June). "The State of Industrial Cybersecurity 2018," in *CXP Group, Nanterre, France* [Online]. Available: https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf.

[4] P. Dreyer. (2018, Jan. 15). "Estimating the Global Cost of Cyber Risk: Methodology and Examples," in *RAND Corporation, Santa Monica* [Online]. Available: https://www.rand.org/pubs/tools/TL281.html.

[5] M. Riek, R. Böhme, et al. (2016). "Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries," in *Delft University of Technology, Netherlands* [Online]. Available: https://repository.tudelft.nl/islandora/object/uuid%3A72a74f3b-94eb-41ca-992b-8d29977ab4d1#.

[6] S. Romanosky, "Examining the Costs and Causes of Cyber Incidents", in *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121-135, December 2016. [Online]. doi: https://doi.org/10.1093/cybsec/tyw001.

[7] S. Morgan. (2016, Feb. 6). "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics," in *Cybersecurity Ventures* [Online]. Available: https://cybersecurityventures.com/cybersecurity-almanac-2019/.

[8] Networking & Information Technology Research & Development Program. (2018, March 22). *Framework for Improving Critical Infrastructure Cybersecurity* [Online]. Available: https://www.nitrd.gov/nitrdgroups/images/6/66/Cybersecurity_Framework_03222018.pdf.

[9] National Institute of Standards & Technology. (2014, September). "Guidelines for Smart Grid Cybersecurity," in *Maryland, NISTIR 7628, rev. 1, vol. 1* [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

[10] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid*. Rockland, Massachusetts: Syngress Media, 2013.