EENA Technical Committee Document

Security and Privacy Issues in NG112

Title:	Security and Privacy Issues in NG112		
Version:	1.0		
Revision Date:	01-06-2017		
Status of the document:	Draft	For comments	**Approved**

EENA
info@eena.org - www.eena.org

Authors and contributors to this document

This document was written by members of EENA:

Authors	Country / Organization
Bill Mertka	USA, Motorola Solutions, Inc.

Contributors
EENA Technical Committee

Legal Disclaimer

This document is authored by EENA staff members with contributions from individual members of EENA and represents the views of EENA. This document does not represent the views of individual members of EENA, or any other parties.

This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.

Table of contents

1 Executive Summary

This document was written as an introduction to the security and privacy concerns surrounding the implementation and rollout of NG112 technology and services. Some of the major conclusions / recommendations discussed in the document include:

- Transition of emergency networks and citizen-to-authority communications globally from traditional telephony technology to IP-based infrastructures brings many benefits, but also challenges
- High on the list of challenges is providing adequate cybersecurity and privacy mechanisms to protect the new infrastructure and the data traversing it
- Security has many aspects, physical, operational, and cyber, but the new challenges for public safety largely lie in the cyber domain
- In the new era, public safety agencies will have to be "cybersecurity savvy" and able to research, develop, and maintain adequate cybersecurity and privacy protection, or know enough to select the proper vendors to provide these services.
- Adequate cybersecurity and privacy protection in the era of IP-based systems involves more than deploying security systems technology like firewalls and intrusion detection systems
    - Policy, operational procedures, threat intelligence and assessment and information sharing mechanisms with friendly stakeholders must all be put in place
- ***EVERY*** entity in the public safety services provision ecosystem will have to develop and maintain its own security and privacy controls, based on international standards and best practices to the extent possible and developed in coordination with other stakeholders
- Successful plans, procedures and systems will involve some basic steps:
    - Set a vision
    - Sharpen your priorities
    - Build the right team
    - Enhance your controls
    - Monitor the threat.
    - Plan for contingencies
    - Transform the culture

2 Introduction

Globally, cybersecurity and privacy are two of the most important topics and concerns in communications technology. It seems like every day there is a new story about hacking, data theft, denial-of-service (DOS) attacks and other cyber and privacy breaches that leave no sector immune, no institution or individual untouched. The transition to open, globally interconnected packet-switched networks has flattened communications infrastructures, drove more efficient communications, and, coupled with revolutions in the affordability and portability of computing power, ushered in a multimedia communications revolution. But this transition has had a dark side, the one referred to above. Openness for greater communications efficiency also means open for "nefarious actors" to disrupt, interrupt, and steal communications and information. Public safety will not be immune from this dark side as it, too, transitions to open, packet-based communications away from closed telco networks and implements the technology necessary to accept multimedia content from the general public and not just a traditional "phone call." This paper will touch briefly on what cybersecurity is, and the need for Public Safety Answering Points (PSAPs), public safety authorities and their governing bodies to be aware of its bedrock concepts, the impacts of deploying it on operations, and the implications the coming transition will have on both communications and information security.

Before getting into the particulars surrounding "cybersecurity and privacy concerns" in NG112, a review of the communications revolution that led to the development of NG112, and just what NG112 is, is in order. It is, as well, important to note, that while this paper is written with the European market in mind, the problems of cybersecurity and privacy protections are really global in nature. In today's interconnected world, cyber attacks and security breaches can come from halfway around the world as easily as the can from next door. Managers of 112 systems and facilities should rightly be concerned by this fact, but should also take comfort in knowing that solutions to this global problem are being worked on across the world and solutions can, and will, come from many different sources.

3 The Internet: A Global Communications Revolution

Since the mid 1990's, the world has undergone a communications revolution sparked by the commercialization of the Internet, a computer communications network originally designed in the 1960's in the United States to foster survivable communications networks in times of national disaster. In the mid-1990's, this network, until then largely the domain of defense and research institutions, was commercialized and the rest, is, as they say, history. Global communications networks arose swiftly, based upon the standards used by the Internet (so-called "IP networks") and transformed global communications into the form we know them today. The growth of a globally standardized, packet-based communications medium, originally used for data, and now almost universally for voice traffic as well, transformed virtually every sector of the global economy, ushering in an era of inexpensive, efficient and increasingly high-bandwidth communications.

The introduction of the "smartphone" early this century, most typically exemplified by the introduction of the iPhone by Apple in 2007, mobilized the Internet and IP-based communications and transformed how people communicate with each other, at a pace more rapid than the enterprise IP revolution of the late 1990's. People could now freely communicate with each other using voice, text, image and video information and a host of new data-focused social medial platforms. People and organizations today communicate more richly and frequently, than any generation in history and these trends are only accelerating. One of the few sectors largely untouched by the global communications revolution was public safety. Starting early in this century, however, efforts to introduce "next generation" technologies to the public safety arena proceeded in earnest and EENA , in Europe and increasingly around the globe, has led this effort in concert with other global organizations like NENA in North America. The introduction of standards for "NG112," closely related to those for NG9-1-1 promulgated in North America, has the potential to transform the public safety sector, especially in the realm of citizen-to-authority communications, like IP networks and smartphone technology has transformed other sectors.

4 NG112: What Is It?

It is estimated that 320 million emergency calls are made every year in the European Union, enabling emergency services to assist citizens in all sorts of difficult situations. All over the world, citizens expect to be able to contact emergency services with technologies they use to communicate every day. Thus, European

citizens have clear expectations about the availability of 112 emergency services with enhanced capabilities of technologies being used in daily life. However, the existing, legacy emergency services infrastructure (circuit switched telephony for 112 telephone calls, not data) is not designed in a way that enables interaction with enhanced services, or that current and future communications and operational requirements will be met. Simply put, the emergency services infrastructure has not kept up with technology, thus, is not able to provide the level of service that citizens expect. Hence, a new technology with a new architecture is needed to resolve these issues– the "Next Generation 112 architecture (NG112)." NG112 enables citizens to contact emergency services in different ways, using the same types of technology as those they use to communicate every day. It also makes possible that 112 PSAPs receive more and better information about emergencies of all magnitudes and improves interoperability between emergency services. Consequently, response time and operation cost will be reduced, while effective response will increase significantly.

NG112 addresses three major objectives:

1. Communication between citizens and emergency services: NG112 is designed to enable citizens to reach an authority (e.g., PSAP) by calls using VoIP, text messaging, real-time text, pictures and video. It could also provide emergency services with more data, such as location and health data. NG112 enables the delivery of calls, messages and data to the appropriate PSAP and other appropriate emergency entities, and adds significant value to the call handling process.

2. Interoperability between emergency services: NG112 enables several Public Safety Answering Points (PSAPs) to be part of a common emergency services IP network, providing them with redundancy and interoperability features. This network should support data and communications needs for coordinated incident management between PSAPs, and provide a reliable and secure environment for emergency communications.

3. Open Standards approach: NG112 is based on Internet Protocol (IP) - network based standard interfaces between all forms of communications components. Existing off-the-shelf hardware and software can be deployed, which increases the technical commonalities between EU member states, drives TCO and fosters the European public safety eco-system. Existing experience from other regions, namely NENA in the US, with its significant work on the NG9-1-1 architecture definition and couple with pilot and certification experience, is carefully examined in the NG112 approach and where necessary, adapted to European needs.

Concluding, the evolutionary path towards NG112 lies in opening emergency services access to the Internet. Besides, access to emergency services is a highly sensitive public safety segment. Thus, equally important to enabling technology, is the fact that NG112 also requires the revision of EU and national emergency services policies, regulations and statutes.[1]

Like other sectors, however, this transition to IP-based networks, an opening to the Internet and rich multimedia communications has not been an unmitigated good. The very open nature of the standards upon which IP communications is built also has become the conduit through which the frequent, and increasingly damaging, cyber attacks we hear about in the news are made. The technology of the Internet, like most technology innovations, is a two-edged sword, the characteristics that make it transformative for good also making it transformative for criminal and destructive behavior as well, the trick, going forward, for those involved with the rollout of NG112 will be to maximize the positive aspects of the NG transition while mitigating its negative consequences.

5 Cybersecurity and Privacy Considerations in NG112

Security and Privacy are at the heart of everything the contemporary IP network revolution, or this should be the case, for several reasons. Understanding the meaning of cybersecurity and privacy protection and their importance is key to successful implementation of these types of protection. Also, understanding the nature of IP networks that makes the so insecure and open to attack is key to understanding why, in the era of NG112, strong cybersecurity and privacy protection technology and operational procedures will be key to reaping the full benefit of the transition.

Perhaps the simplest definition of cybersecurity is supplied by the Merriam-Webster dictionary:

[1] Taken from ***Next Generation 112 Long Term Definition***, v1.1, 03-06-2013, pp. 11-12.

"Cybersecurity is measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack"[2]

A more extensive definition is given in the glossary of the National Initiative for Cybersecurity Careers and Studies (NICCS):

"Definition: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."[3]

Somewhere in between the first, simple definition and the last most comprehensive one lays the sweet spot for public safety with regard to the level of cybersecurity programs and technology that needs to be implemented. Of course in order to truly "protect" the NG112 infrastructure, public safety managers will have to avail themselves of information sourced from all the domains named, in that last, more comprehensive definition.

N""Information assurance" is considered a part of cybersecurity. Privacy protection and considerations, involve both technical means to assure data stored in the system IS what it says it is, and to protect it from unauthorized disclosure. Given that legal, regulatory and policy regimes differ across jurisdictions and determine the "rules" that are put in place to "protect" data privacy, it is hard to make generic conclusions about data privacy. Nevertheless it is an important area tha bears monitoring as rollout of NG112 starts to take place. Data privacy is an area of great concern globally, but of special concern in European Union member countries, where data privacy laws and regulations are strict, and violation penalties severe. The potential problems and issues for NG112 caused by the impact of data privacy in a primarily "data driven" system like NG112 are varied and multiple. They are specially discussed in a later section.

Another way to look at cybersecurity is by viewing it from the perspective of the "business function" it provides. Another helpful definition of "cybersecurity" is:

"Cybersecurity is the business function of protecting an institution from the damage caused by cyber-attacks in the face of constraints such as other business objectives, resource limitations and compliance requirements. It has three facets: risk management, influencing, and delivery."[4]

As the reference text goes on: "Cybersecurity is first and foremost a risk management function – there is NO WAY to prevent all cyber-attacks from occurring."[5] Cyber attacks, intrusions, and data theft WILL happen under NG112, the idea is to be able to balance risks with matching defenses and mitigate or shut them down as soon as they are identified. Influence refers to cybersecurity staff having to "influence" others in the organization to act with cybersecurity in mind, emphasizing the fact that the cybersecurity protection "chain" is only as strong as its weakest link, and delivery refers to what most people think cybersecurity is, i.e., the actual technical means for delivering some modicum of cybersecurity to the public safety system at PSAPs and core sites. This definition nicely captures that the fact that comprehensive cybersecurity depends not only on technical means, but also on policies, procedures, and above all PEOPLE. Poorly trained staff is the NUMBER ONE reason for cybersecurity breaches in all sectors and public safety under NG112 will likely not be any different. Thus the need for vigilance, training, and programs geared toward "upping the cybersecurity quotient" of everyone involved with the public safety service delivery chain.

[2] https://www.merriam-webster.com/dictionary/cybersecurity, accessed 26-02-2017
[3] https://niccs.us-cert.gov/glossary, accessed 26-02-2017
[4] Kaplan, James M, et. al. *Beyond Cybersecurity: Protecting Your Digital Business*. NY, John Wiley and Sons, 2015. PP. xiv – xv.
[5] *Ibid*.

5.1 Cybersecurity and the Successful Rollout of NG112

So why is cybersecurity so important in the rollout of NG112? As discussed above, it is because of the inherently open nature of IP-based networks. IP networks were developed to foster resilient connectivity but not necessarily security. IP multimedia services are easy targets for hackers and information thieves because they are based on IP networks that are inherently insecure. The IP family of protocols was also have been built on top of IP over time. Once the transition to NG112 takes place, public safety organizations will be reliant upon these IP networks to deliver Emergency Services.

Trying to classify and control all of the communications on an IP network is an increasingly difficult task, never mind understanding the content of the various real-time data exchanges going on. Circuit switched networks were designed to connect two points with a physical and unchanging path for the duration of a call. Conversely, IP was designed to route around failures and take the best path between two points. Combining the classification problem with the fact that communications are becoming increasingly ubiquitous and virtual, users do not necessarily know where one another are located or how their information is transmitted on an IP-based packet-switched network.

A quick review of the design principles for the original Internet are very revealing in terms of showing the existence of security "attack vectors" from the very start of the system. Since the system was closed for most of its early existence, however, it was not exposed to the machinations of malicious actors until much later so the existence of these "time bombs" was not apparent at the time. These principles guided the development of the original Internet:

1. Redundant Links
2. No Central Control
3. All Messages broken into equal size packets
4. Variable routing of packets depending on the availability of links and nodes
5. Automatic reconfiguration of routing tables immediately after the loss of a link or a node[6]

The vulnerabilities opened up by these original design principles are the reason cybersecurity and privacy protection are so important to the successful rollout of NG112. The "holes" in the system started to be exposed as soon as it was opened up to the external world and today, in some circles, some researchers have even seen some businesses and processes "backing away" from being "online" due to serious concerns about cybersecurity. The ultimate success of NG112 will depend on successful implementation of cybersecurity and data protection technology and processes.

6 Brief History of the Emerging Challenges in Cybersecurity And Types of Attacks

Obviously, there were NO cybersecurity challenges for public safety in the days before widespread interconnection of computers on data networks. As voice calls became "just another channel" on the data network, the issue of cybersecurity became front and center not just for data networks but for real-time communications like voice as well. A good understanding of the history of emerging cybersecurity challenges and the types of attacks that have evolved is key to understanding what types of threats will exist in the world of "fully implemented" NG112 and give a hint to the types of measures that must be enacted to protect against them.

The term "computer virus" was first defined in 1983, and the first virus to affect personal computers (PCs) came along the first year the IBM PC was introduced to the market, 1981. Threats such as viruses, worms, and Trojans were quick to emerge.

"A computer virus is computer code that is designed to insert itself into other software and, when executed, is able to replicate itself and propagate with host software or file…a worm does not change other programs, but a worm is a computer program that has the ability to replicate itself from computer to computer and to cross over network connections…. [while] a Trojan horse is a program that masquerades as a legitimate application while also performing a covert function."[7]

[6] Johnson, Thomas A., ed. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. Boca Raton, FL: CRC Press, 2015, PP. 6-7.
[7] *Ibid.* PP. 9-10.

Starting in 1981 and progressing through the early decades of the 21st century, cyber attacks grew in scope and severity. The term "cybersecurity" itself is documented as first being used in 1989. So, even before the Internet was commercialized, malicious threats to digitized information processed by computers existed. The rise of the Global Internet only hastened their spread.

6.1 The Information Security Model and Risk Management

The standard model for discussing primary concepts in information security is the CIA model, which stands for Confidentiality, Integrity and Availability. This model was developed by the International Information Systems Security Certification Consortium (ISC^2).

- ***Confidentiality*** is a necessary component of data privacy and refers to the ability to protect data from those who are not authorized to view it.
- ***Integrity*** refers to the ability to prevent data from being changed in an unauthorized or undesirable manner.
- ***Availability*** refers to the ability to access data when it is needed.

Attack approaches and vectors can best be understood within the context of this model. Attacks can be broken down according to the type of attack is represented, the risk the attack represents, and the controls that can be used to mitigate the attack.

Attacks can generally be placed into one of four (4) categories: interception, interruption, modification, and fabrication. Each category can affect one or more of the principles of the CIA triad as shown in Figure 1 below.

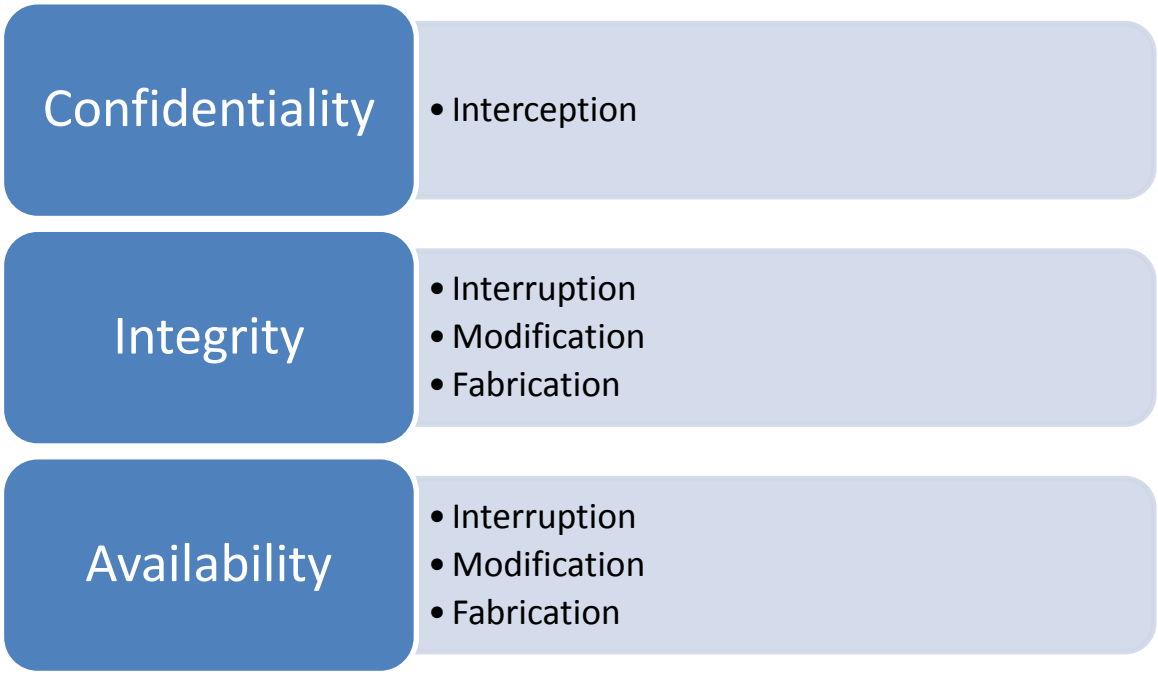


Figure 1: Categories of Attack

Interception attacks allow unauthorized users to access data, applications, or environments, and are primarily an attack against confidentiality.

Interruption attacks cause assets to become unusable or unavailable for use on a temporary or permanent basis. Interruption attacks often affect availability but can be an attack on integrity as well. For example, a DDOS attack on a mail server would be classified as an availability attack.

Modification attacks involve tampering with assets. Such attacks might primarily be considered an integrity attack but could also represent an availability attack.

Fabrication attacks involve generating false data, processes, communications, or other similar activities with a system. Fabrication attacks primarily affect integrity but could be considered an availability attack as well.

Other key concepts regarding security threats to information and communications systems are:

Threat: a threat is something, a virus, a worm, botnet, etc, that have the potential to cause harm to a system.

Vulnerabilities are weaknesses' that can be used or exploited to harm a system. They are "holes" that can be exploited by threats to harm a system or network.

Risk is the likelihood that something bad will happen. In order for risk to exist, both a threat and a vulnerability that threat can exploit needs to exist.

All this points to the fact that modern cybersecurity protection, as mentioned, is an exercise in risk management; one cannot protect against ALL threats, so the task of security breach mitigation much balance identification of threats, assessment and eradication, where possible, of vulnerabilities, and available resources. The risk management process is really a cycle that involves the following steps:

1. Identify the Assets to be protected
2. Identify existing and possible future threats
3. Asses existing and possible future vulnerabilities
4. Assess risks
5. Mitigate risks.

This continuum is depicted in Figure 2:

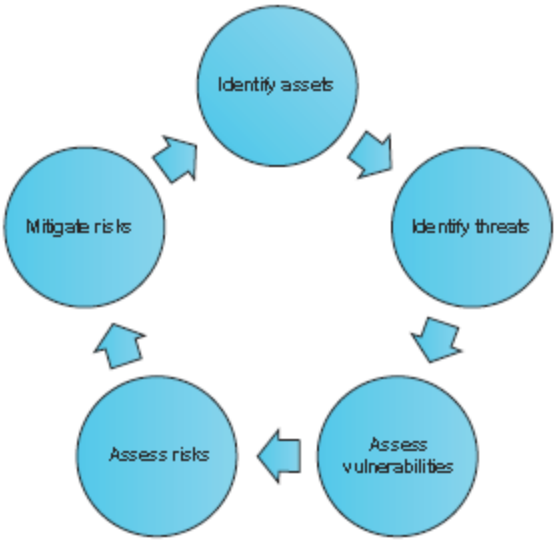
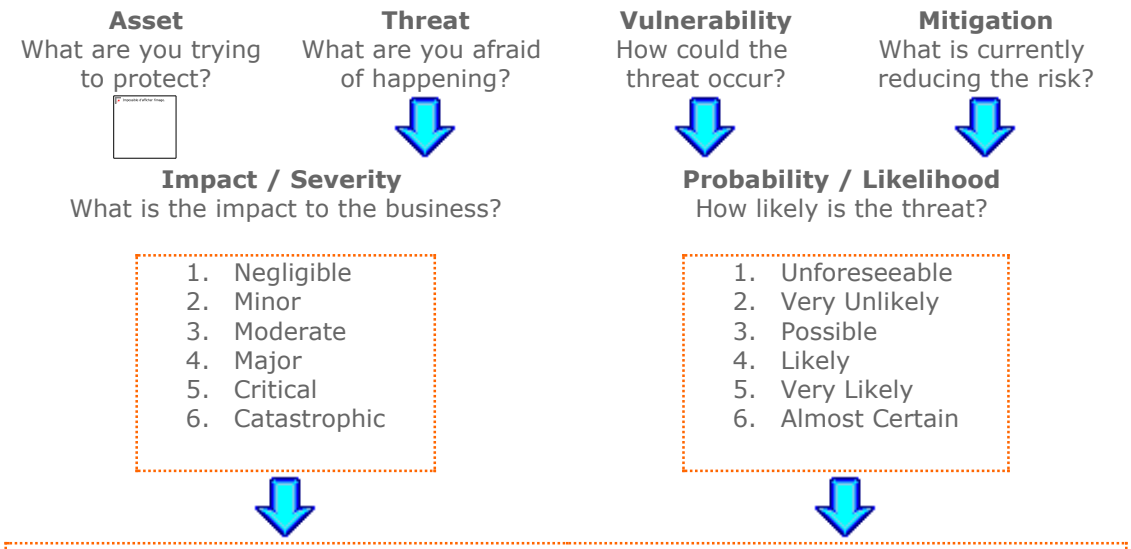


FIGURE 2: Risk Management Process[8]

Within a risk management framework, once the risks are identified, one should assess the risks from both a customer and process perspective. A basic risk assessment process would rank each risk based on financial impact and likelihood of occurrence. Sometimes a risk log or matrix is a good place to start.

An example can be found online at http://www.ruleworks.co.uk/riskguide/security-risk-log.htm[9]

[8] This discussion of the information security model and attack types is taken from Andress, James. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, Second Edition. Waltham, MA: Elsevier, 2014, pp. 5-13.



Risk Log

Risk Log - Example of Security Hazards				Tolerability Level 12
Priority	Hazard	Impact (1-6)	Probability (1-6)	Risk Rating (Impact * Probability)
1	Data loss due to virus attack	5	4	**20**
2	Denial of Service attack	5	3	**15**
3	Theft of proprietary information	4	3	**12**
4	Insider net abuse	4	3	**12**
5	Abuse of wireless networks	3	4	**12**
6	Financial fraud	5	2	10
7	Laptop theft	3	3	9
8	Unauthorized access	3	3	9
9	Telecom fraud	2	3	6
10	Web site defacement	3	2	6
11	System penetration	3	2	6
12	Sabotage	4	1	4

The risk assessment should be use to place risk events in one of four risk response categories:

- ***Reduce or Mitigate risk*** – activities with a high likelihood of occurring, but financial impact is small.
- ***Avoid risk*** – activities with a high likelihood of loss and large financial impact. The best response is to avoid the activity.
- ***Transfer risk*** – activities with low probability of occurring, but with a large financial impact. The best response is to transfer a portion or all of the risk to a third party by purchasing insurance, hedging, outsourcing, or entering into partnerships.
- ***Accept risk*** – if cost-benefit analysis determines the cost to mitigate risk is higher than cost to bear the risk, then the best response is to accept and continually monitor the risk.

Risk mitigation involves putting measures in place to help insure that a given type of threat is accounted for. These measures are referred to as controls. Controls can be physical, logical and administrative.

[9] This section is based upon the NENA draft document *Introduction to NG9-1-1 Security*.

Physical controls are those controls that protect the physical environment in which systems are installed or data is stored. Such controls also involve controlling human access into and out of such environments. Physical controls include such items as fences, gates, locks, bollards, guards, and cameras.

Logical and technical controls are those that protect the systems, networks, and environments that process, transmit, and store data. They can include such systems as passwords and other identification and authentication tools, encryption, logical access controls, firewalls, and intrusion detection systems. An overview of technical means of control is included later in this paper.

Administrative controls are based on rules, laws, policies, procedures, guidelines and other items that are "paper" in nature. Administrative controls set out the rules for users of a system to behave. One shortcoming of administrative controls, however, is the ability, or lack thereof, to enforce them. IF the organization promulgating them does not possess the authority to enforce them they are worse than useless.

6.2 Incident Response[10]

In the event risk mitigation efforts fail, incident response exists to react to such events. Reaction to security incidents should be based, as much as possible, on documented incident response plans. The incident response process consists of:

- ***Preparation*** – The preparation phase of incident response consists of all the activities that can be performed in advance of any actual incidents, the enable better handling of the events once they occur. The importance of good preparation cannot be underestimated. Public safety entities MUST know, to the extent feasible and possible, HOW they will react if any of the threats outlined above affect their center. Without adequate planning and preparation, no incident response will go well.
- ***Detection and Analysis*** – Detection is where the action starts, where incidents are identified as a result of monitoring or alerting based on the output of a security service or tool, such as an Intrusion Detection System (IDS), Anti-Virus (AV) software, firewall, proxies and a review of their logs, alerting from a Security Information and Event Monitoring (SIEM) tool if is it internal or by a service run by a Managed Security Services Provider (MSSP). Analysis, which can be automatic or manual, consists in trying to determine whether a detected issue constitutes a security incident or not. If an incident is deemed to have occurred, containment, eradication, and recovery operations will commence.
- ***Containment*** – Containment involves taking steps to insure that an incident does not cause any more damage than it already has, or to at least lessen any ongoing harm.
- ***Eradication*** – During the Eradication phase, attempts are made to remove the effects of the incident from the protected environment.
- ***Recovery*** – After eradicating the threat / security breach, the system needs to be recovered, or put into a better state than it was in prior to the incident, or at least the state that existed prior to the discovery of the incident. This involves restoring devices and data from backup media, rebuilding systems, reloading applications, or any number of similar activities. In addition, the attack vector used need to be mitigated.
- ***Post-Incident Activity*** – Also called a "post-mortem," after the incident has passed, an attempt should be made to specifically determine what happened, why it happened, and what can be done to keep it from happening again.

6.3 Types of Cybersecurity Attacks

Today's threat landscape has grown in size and severity from the early days of information security outlined above. Today's potential threats encompass the following laundry list of attack types:

Phishing and Spear-phishing – Attacks delivered via familiar-looking e-mail, either broadcast (phishing) or targeted ("spear-phishing")

Advanced Persistent Attacks (APTs) – Sophisticated network attacks in which the attacker seeks to gain information and remain undetected for a substantial period of time…APT attacks are not designed to do damage, but to acquire information or modify data.

[10] Discussion of incident response is based upon Andress, *Op. Cit.*, pp. 16-18.

Zero-day Vulnerabilities – Attacks that use identified, but previously unused vulnerabilities in applications, operating systems, etc. Since the "zero day" vulnerability is unknown out in "the wild," no software patch or hardware fix yet exists to "fix" the vulnerability. "Zero day" vulnerabilities are among the most highly sought after items in the hacking and cyberwarfare world, with hackers and governments willing to pay significantly for "zero days" around which future cyber attacks and cyberweapons can be built.

Rootkit tools and attacks – Rootkit attacks are based on a set of tools that enable root- or administrative-level access to a computer system. Rootkit has become synonymous with term malware and is used to describe malware with rootkit capabilities.

Malware and Mobile Malware - Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses, and spyware. Malware is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising and was first defined in 1990. Mobile malware is malware which contaminates mobile devices like smartphones and tablets. **Ransomware** is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.[11]

Bots and Botnets – Distributed Denial of Service Attacks (DDOS), etc. – A botnet is a network of compromised computers that can be coordinated remotely a cybercriminal or attacker to achieve a malicious purpose. The malicious goal may range from initiating a distributed denial-of-service attack, spam attack, click fraud attack, or simply renting out an attack service to individuals who may want to have some other person or entity attacked. In a DDOS attack, the compromised machines in the botnet are all directed to attack a predetermined victim, corporation or government entity at s specific time and date.[12]

With regard to the limited resources available on public safety and other IP-based networks, overload happens when all the available resources are consumed, or there is a significant impact to the performance or availability of a network. Intentional overloads, as has been discussed, can be malicious denial of service or distributed denial of service events, which are referred to as DOS or DDoS attacks. These are conducted over the IP network, or even automated and brought in over the telephony network to tie up trunks (in which case they are called TDOS or Telephony Denial of Service attacks). In the world of IETF Session Initiation Protocol (SIP) communications it's most common to see invite (i.e., SIP INVITE method) or registration (i.e., SIP REGISTER method) floods from the Internet since these tie up both bandwidth and telephony resources. DOS attacks are very difficult to stop since the attacker can shield themselves by using many servers or workstations that they have previously compromised and taken control of during a single attack. Social networks are also being used to coordinate focused attacks by willing parties.

7 Review of Current Security and Privacy Technology Solutions[13]

Having completed overviews of what cybersecurity is, how it might be carried out at the policy and procedure level, and the clear need for such systems to protect what is understood, or should be understood, to be "critical infrastructure," it is germane to next turn to some of the tools used to provide the protections and cybersecurity "incident response" discussed above. The sub-sections of this part of the document briefly describe the characteristics of some of the more common security technologies and solutions that make up the physical infrastructure of a cybersecurity protection system.

7.1 Antivirus (AV) software

Antivirus software grew out of the reality that traditional computer operating system design paradigms were not able to stop "viruses" from "infecting" computer systems. Today's virus checkers rely primarily on "signatures:" they match files against a database of code snippets of known viruses. The code matched can be part of the virus' replication mechanism or its payload. The disadvantages of this sort of pattern-matching approach should be obvious. Unless you have some of the virus code signatures in the database, the AV software can't scan for them, so if virus developers obfuscate or otherwise try to hide virus signatures, or AV databases are not kept up to date, viruses will be missed by the checker. A second approach, used somewhat

[11] Ransomware definition from https://www.trendmicro.com/vinfo/us/security/definition/Ransomware, viewed 04-03-2017.
[12] Attack list and definitions taken from Johnson, ed. *Op. cit.,* pp. 11-17.
[13] The discussion inc Chapter 9 is almost entirely taken from Bellovin, Steven M. *Thinking Security: Stopping Next Year's Hackers*. NY: Addison-Wesley, 2016, pp. 45 – 201.

today but likely to be a mainstay in the future, relies on anomaly detection. Anomaly detection relies on statistics; the properties of normal programs and documents are different than those of malware; the trick is to avoid false positives.

Antivirus software is not a fire-and-forget technology; it needs constant attention, both because of the changing threat environment and the changing computing environment. The need for up-to-date signature and anomaly databases should be quite clear. One of the most controversial issues surrounding AV software is on which machines it should be used. AV should be understood as one line of defense in a multi-layered defense system (which is discussed in more detail later in this paper). It protects against threats that an OS cannot catch, and it is also capable of blocking attacks that somehow managed to get through another protection layer. AV, more properly anti-malware, software is a mainstay of today's security environment. Unfortunately, it is losing its efficacy.

So, should you run AV software in your environment? For generic desktop systems, the answer is probably yes. It's relatively cheap protection and is usually trouble free. Similarly, server or firewall-resident scanners can block malicious inbound malware before it reaches users. All this is depends, though on keeping AV databases updated regularly.

7.2 Firewalls and Intrusion Detection Systems

Since the dawn of the commercial Internet, firewalls have been a mainstay of security defense. That said, their utility, and in particular the protection they provide, has diminished markedly over the years. The original purpose of firewalls was to keep "bad guys" away from bugs inherent in internal computer code that could be exploited, but in a world awash in malware, phishing attempts, and the like, the original theory and use for a firewall is being challenged like never before. A firewall traditionally was a security policy enforcement device that takes advantage of a topological chokepoint. There are three properties necessary for a firewall to be effective:

1. A topological chokepoint must exist at which to place a firewall.
2. The nodes "inside" of the firewall share the same security policy
3. All nodes "on the inside" must be "good;" all nodes on the outside are, if not actually "bad," untrusted.

When one or more of these conditions cannot hold, a firewall cannot succeed. Today, none are true for the typical enterprise, including the (coming) IP-connected PSAP, unless of course the network to which the PSAP is connected is completely walled off from the Internet which would, unfortunately, defeat the entire promise and purpose of migrating to NG112 networks and systems! It is worth noting, however that with the exception of #3, none of these are absolute. Minor deviations in #1 or #2 are tolerable. But any deviation from these principles will limit the effectiveness of a firewall. It is also important to realize that no firewall can provide protection at any other layer of the protocol stack other than the one in which it operates. For example, a typical packet filter operates at layer 3 and a bit of layer 4 (the port numbers) and, as such, can filter by IP address and TCP port. It can't look at MAC addresses nor can it look inside e-mail messages. All of this has made today's firewalls more complex. Thus, regarding firewalls, some conclusions can be drawn:

- Small-scale firewalls, protecting a network about the size run by a single system administrator, still serve a useful function.
- Complex server applications are rarely amenable to firewall protection, unless the firewall has some very, very good (and very well written) sanitizing technology
- An enterprise firewall retains value against low-skill attackers but is actually a point of risk, not protection, when trying to filter complex protocols against sophisticated adversaries.
- Mobile devices, in general, should never be fully trusted, because of their likelihood of carrying malware.

An ***intrusion detection system*** (IDS) is a backup security mechanism. It assumes that your other defenses – firewalls, hardened hosts, etc. – have failed. The task then is to notice a successful attack as soon as possible, which permits minimization of the damage. Like AV software, IDS's can be signature or anomaly based; the same advantages and disadvantages apply. The key difference is in deployment scenarios; AV software operates on files and IDS's are generally classified as network or host intrusion detection systems. Host IDS's can operate on network or host behavior or content. Both the network and host IDS approaches has plus's and minus's. the big attraction of anything network based is scalability; like a firewall a network IDS, many times installed on the same network element hosting the firewall, can watch over a network where many hosts are connected. The idea is to grab packets as they traverse the network ingress, scanning IP

addresses and port numbers, looking for anomalies. Dealing with encrypted traffic is an issue and the possibility of missed packets also exists with network-based IDS. The fundamental problem with any form of network IDS is that it lacks context. It is difficult for even the best network scanners to re-assemble every packet in transit and then scan it for malware. This is much easier done on host IDS systems. Hosts can also look at log files, all but impossible to do at the network level, and can scan their own file systems for unexpected changes. Host-based IDS can also emulate network protocols, above the level of any encryption. There also specialized IDS systems that are aimed at so-called "extrusion detection," or trying to detect someone explicitly trying to steal your data and "extract" it out of your system.

An ***intrusion prevention system*** (IPS) can be described as an IDS that is also equipped to do some remediation if an anomalous security event is detected. An IPS can do many things; as with an IDS, it can host or network resident; both have advantages and disadvantages. Depending on where it is located, it can block connections, quarantine files, modify packets, and more. The good functioning of an IPS rest on three foundations: very good detection, selection of countermeasures, and matching the countermeasures to confidence in identification of the root cause of the problem. For this reason, IDS and IPS systems are integrated into an IDS / IPS.

7.3 Cryptography and VPNs

The two most common uses of ***cryptography*** are to prove identity and to hide data from those who are not authorized to see it. It can do these things very well, but at a price, the most obvious being the encrypting keys have to be protected. When keys are exposed, the cryptography employed is rendered useless. A second major challenge to employing cryptography for information security is the difficulty encountered of devising proper cryptographic mechanisms. Cryptography is a very difficult and subtle branch of applied mathematics; remarkably few people are qualified to practice it. NEVER use a proprietary encryption algorithm, especially if you are told that it's more secure because it is secret. The story of SSL 3.0 and the TLS protocol derived from it, are warning enough here.[14] A third issue with cryptographic-based security is that it is very difficult to retrofit cryptographic methods to existing systems, especially if there are complex communications systems or requirements. Ideally, cryptographic methods should be designed together with the system they are intended to protect. Unfortunately, "Greenfield" systems are rare. The two primary ways encryption is deployed in a system is *transport encryption*, where a real-time transport channel is being protected, and *object encryption*, where data must be protected across an arbitrary number of hops amongst arbitrary parties. You should always use authentication with encryption; there are too many games an attacker can play if you don't. The most common layer of the protocol stack where transport encryption is done is at the application layer (Layer 7). In particular, TLS and it older sibling SSL are heavily used for web transmission security and TLS is written into the NG112 specification. Object encryption is much harder than transport encryption because by definition you are not talking to another party when you encrypt something. Since a lost key has serious implications for object encryption, one should avoid using it unless the risk to the data you want to protect is VERY great.

Virtual Private Networks (VPNs) are intended to provide seamless, secure communications between a host and a network or two or more networks. The big advantage of VPNs is they provide "fire-and-forget" cryptography; once you turn one on, all of your traffic is protected. Although many VPN topologies exist, only two are common: connecting multiple locations of a single organization and connecting mobile devices back to the enterprise network. A VPN is intended to seem and operate like a real network, with one crucial difference; some of the "wires" of the network are in fact encrypted network connections that may pass through many other networks and routers. These links, or tunnels, are often treated like any other network links. Picking what VPN technology to use is harder than deciding that you need one. There are at least FIVE obvious choices: IPSec, Microsoft's Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), the IETF version of PPTP that needs to run over IPSec to be secure, OpenVPN, and a larger group of so-called "TLS (or SSL) VPN" products of which there are TLS portal and tunnel VPNs. IPSec has the cleanest architectural vision. It is available on virtually all platforms, supports a wide range of authentication methods, and can secure more less anything layered on top of it.

Overall, protecting cryptographic keys is extremely important to using cryptographic security methods. Strong overall security will require different keys for different security levels, suitable software to let users manage such complexity, and a lot of user education and training on how to behave.

[14] See Bellovin, Steven M. *Op. Cit.*, pp. 82 – 83.

7.4 Passwords and Authentication

Authentication is generally considered to be one of the most basic security principles. Absent bugs, authentication effectively controls what system objects someone can use. In other words, it is important to get authentication right. There are three (3) basic forms of information that can serve as the basis of an authentication system: something you know (e.g., a password), something you have, such as a token or a particular mobile phone, or something you are, that is some form of biometric.

The classic authentication method, passwords, has generated and continues to generate discussion how best to employ them and how actually effective they are. The need for strong, un-guessable passwords, clashes with usability of systems in the real world, and realistic systems try to balance both imperatives. As the threat model has changed, ideas about what constitutes the "best passwords" has changed with it. What type of password discipline to enforce depends on the answers to certain questions about your system design:

1. What types of guessing attacks are you trying to guard against, online (where the attacker actually tries to login) or offline, based on a stolen hashed password file?
2. Are the passwords in question employee passwords or user passwords?
3. More generally, are you concerned with opportunistic or targeted attacks?
4. What do you assume the enemy can do? Subvert client machines? Subvert your servers? Launch phishing attacks? Bribe employees? Eavesdrop on conversations?

Some commentators think biometric authentication systems might be a solution to the password conundrum, but consider this: a biometric authentication system consists of a number of components: a human, a sensor, a transmission mechanism, a biometric template database, and an algorithm at a minimum. An attack can target any one of these, which means that they must all be protected. Biometric authentication also involves the thorny issue of privacy. A biometric identifier is more or less the ultimate form of Personally Identifiable Information (PII). Using biometric authentication unnecessarily not only puts you at risk to violate privacy laws, it also exposes organizations to serious public relationship problems should the signature database be stolen. The decision to use biometric authentication should not be taken lightly.

Tokens, something you have, are a popular authentication mechanism for security-sensitive organizations. Using tokens avoids all of the weaknesses of passwords, but they can be more expensive (tokens cost money), and it may be unknown whether all relevant applications in an environment can be adapted to use tokens. Perhaps the biggest incompatibility is the mismatch between applications that instantiate many session over time and the single-use property of most token-based systems.

While no one authentication system is suited for meeting all requirements, all of the time, some conclusions, or observations, about passwords can be drawn from this brief consideration of authentication technologies:

- Passwords are not suitable, ideally, for high-security needs. Making plans to move away, or beyond, passwords makes sense in these environments if the threat model indicates passwords will be a weakness.
- That said, passwords are not going away anytime soon, since converting applications to stronger authentication methods will be, if nothing else, time consuming. In the interim, as the switch is made to stronger authentication methods, use of password managers (do your homework on which one is best for your needs) will help with password reuse and strength problems.
- Implement bilateral authentication; it's strong protection against phishing. Some password managers do this automatically; they will send a password only they recognize the site and they are not fooled by clever e-mail messages
- Master passwords are especially crucial and need the best protection. These, for sure, need to be as strong as possible.
- Plan for exceptions; know in advance how you will handle lost or stolen passwords, compromised servers, and the like.

It is important to note is that there are fads in authentication that go in and out of style over the years. Each organization should decide on the best authentication technology that matches is particular threat mode and operational environment. Perhaps the "one to watch" in the next few years is the single sign on, or "federated" approach to authentication. Both the TFOPA WG1 Final and Supplemental Reports, referred to

earlier in this document, have a good discussion regarding efforts at the US Federal level to address the need for better authentication methods in public safety and well worth reviewing from this standpoint.[15]

7.5 PKI: Public Key Infrastructures

PKI, or public key cryptography, originally described in 1976, is a security method using encryption keys to send secure messages. Someone uses your available and published public key to encrypt a message to you, and you, in turn, use your private key to decrypt it. The trick to making PKI-based security work is how cipher keys are distributed and how the systems that provide them are themselves administered and secured. In 1978, the method of using "certificates," a digitally signed message containing a user's name and public enciphering key, was devised to exchange public keys. Today, certificates are embedded in a framework known as Public Key Infrastructure, or PKI. The Internet Security Glossary defines PKI as "The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography." Proper functioning PKI is about more than just code; it is a SYSTEM. Most PKI certificates use the X.509 standard and are very complex in nature. The fundamental questions about certificates are about security: who signs the certificates? Do you trust them? Are they honest? Are the competent, both at procedures and technically? These questions, and their answers, lie at the heart of a well-functioning security system based on PKI.

When you use a certificate in this way, you are relying on the trustworthiness of the issuer. The heart of the certificate system is the certificate authority, or CA. A CA does just what the name implies, i.e., issues certificates. The crucial limitations of certificate-based systems include:

- It is rarely clear to system administrators or developers which CAs are trusted for given applications. It is almost never clear to end users.
- It is rarely clear to anyone what a given certificate's intended use is.
- It is almost never clear how trustworthy or competent a CA is.

All this indicates that standard Internet-wide PKI as it exists today is unacceptably insecure; however, most of the tools and pieces of a PKI-based infrastructure can be used quite securely if the three problems identified above are addressed. That is, if a scenario can be devised in which everyone knows exactly WHO can issue a certificate and what the purpose of that certificate is and if the issuers can be trusted to an extent commensurate with the resource being protected, you can have a secure (or secure enough) system while using the same software, syntax, etc. of existing X.509 certificate-based systems. This avoids the major issue with web-based PKI systems that exists today, namely the "let a hundred CAs bloom" approach of browser and OS vendors. Trustworthiness is the key issue in PKI and one must limit the number of "trusted CAs" in order for real trust to be established.

7.6 Security Incident and Event Management (SIEM) Systems

According to Gartner: **Security information and event management (SIEM)** technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.[16] Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security. The acronym is pronounced "sim" with a silent e. The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations and being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary. SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system.

A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly. A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting. By bringing these two functions together, SIEM systems provide quicker identification, analysis and recovery of security events. They also allow compliance managers to confirm they are fulfilling an organization's legal compliance requirements.

[15] See TFOPA WG1: Optimal Cybersecurity Approach for PSAPs, *Final Report*, 10 December 2015, pp. 9-12 and 19 -23 and *Supplemental Report*, 2 December 2016, pp. 22-27.
[16] See http://www.gartner.com/it-glossary/security-information-and-event-management-siem/, viewed 06 March 2017.

A SIEM system collects logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment -- and even specialized security equipment like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. To allow the system to identify anomalous events, it's important that the SIEM administrator first creates a profile of the system under normal event conditions. At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event log entries. In some systems, pre-processing may happen at edge collectors, with only certain events being passed through to a centralized management node. In this way, the volume of information being communicated and stored can be reduced. The danger of this approach, however, is that relevant events may be filtered out too soon.

SIEM systems are typically expensive to deploy and complex to operate and manage. While Payment Card Industry Data Security Standard (PCI DSS) compliance has traditionally driven SIEM adoption in large commercial enterprises, concerns over advanced persistent threats (APTs) have led smaller organizations to look at the benefits a SIEM managed security service provider (MSSP) can offer. [17]

7.7 Threat Intelligence and Analytics

Gartner has defined threat intelligence as: "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard[18]. Threat intelligence, also known as cyber threat intelligence (CTI), is organized, analyzed and refined information about potential or current attacks that threaten an organization. The primary purpose of threat intelligence is helping organizations understand the risks of the most common and severe external threats, such as zero-day threats, advanced persistent threats (APTs) and exploits. Although threat actors also include internal (or insider) and partner threats, the emphasis is on the types that are most likely to affect a particular organization's environment. Threat intelligence includes in-depth information about specific threats to help an organization protect itself from the types of attacks that could do them the most damage. In a military, business or security context, intelligence is information that provides an organization with decision support and possibly a strategic advantage. Threat intelligence is a component of security intelligence and, like SI, includes both the information relevant to protecting an organization from external and inside threats as well as the processes, policies and tools designed to gather and analyze that information. Threat intelligence services provide organizations with current information related to potential attack sources relevant to their businesses; some also offer consultation service[19].

IBM defines cyber threat analytics as: "a human-led process that enriches existing security measures with contextual insights gained from external and internal data sources. Defensive weak spots are just waiting to be found and exploited by persistent cyber attackers. But with cyber threat analysis, you quickly identify, disrupt and mitigate breaches by uncovering critical insights unseen by traditional defenses. These insights help identify the who and why behind a threat – and expose seemingly normal day-to-day activity as abnormal and dangerous. The right combination of multi-dimensional analysis capabilities and advanced analytics can help turn defensive cyber strategy into a proactive one – and counter and mitigate more threats."[20] Threat analytics services and solutions take data from threat intelligence providers and help organizations discover, visualize, and communicate meaningful insights from a variety of sources. These sources could be from the private feeds, to open-source data, to network logs, enterprise data, and social media. Cyber threat intelligence platforms and cyber threat analytics platforms work together to provide a more proactive approach to defending against the unpredictable cyber threat landscape

7.8 The Security Operations Center (SOC)[21]

The SOC is where all of these technologies and capabilities come together to help organizations, however they obtain SOC services (see MSSP below), manage and maintain their security environment. A **security operations center** (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect,

[17] This section taken from http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM, viewed 06 March 2017.
[18] See https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/, viewed 06 March 2017.
[19] Taken from http://whatis.techtarget.com/definition/threat-intelligence-cyber-threat-intelligence, viewed 06 March 2017.
[20] See http://www.ibmbigdatahub.com/infographic/what-cyber-threat-analysis, viewed 06 March 2017.
[21] This section is reproduced from https://digitalguardian.com/blog/what-security-operations-center-soc, viewed 06 March 2017.

analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with organizational incident response teams to ensure security issues are addressed quickly upon discovery.

Security operations centers monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

Rather than being focused on developing security strategy, designing security architecture, or implementing protective measures, the SOC team is responsible for the ongoing, operational component of enterprise information security. Security operations center staff is comprised primarily of security analysts who work together to detect, analyze, respond to, report on, and prevent cybersecurity incidents. Additional capabilities of some SOCs can include advanced forensic analysis, cryptanalysis, and malware reverse engineering to analyze incidents.

The first step in establishing an organization's SOC is to clearly define a strategy that incorporates business-specific goals from various departments as well as input and support from executives. Once the strategy has been developed, the infrastructure required to support that strategy must be implemented. According to Bit4Id Chief Information Security Officer Pierluigi Paganini, typical SOC infrastructure includes firewalls, IPS/IDS, breach detection solutions, probes, and a security information and event management (SIEM) system. Technology should be in place to collect data via data flows, telemetry, packet capture, syslog, and other methods so that data activity can be correlated and analyzed by SOC staff. The security operations center also monitors networks and endpoints for vulnerabilities in order to protect sensitive data and comply with industry or government regulations.

The key benefit of having a security operations center is the improvement of security incident detection through continuous monitoring and analysis of data activity. By analyzing this activity across an organization's networks, endpoints, servers, and databases around the clock, SOC teams are critical to ensure timely detection and response of security incidents. The 24/7 monitoring provided by a SOC gives organizations an advantage to defend against incidents and intrusions, regardless of source, time of day, or attack type. The gap between attackers' time to compromise and enterprises' time to detection is well documented in Verizon's annual Data Breach Investigations Report[22], and having a security operations center helps organizations close that gap and stay on top of the threats facing their environments.

Many security leaders are shifting their focus more on to the human element than the technology element to "assess and mitigate threats directly rather than rely on a script." SOC operatives continuously manage known and existing threats while working to identify emerging risks. They also meet the company and customer's needs and work within their risk tolerance level. While technology systems such as firewalls or IPS may prevent basic attacks, human analysis is required to put major incidents to rest.

For best results, the SOC must keep up with the latest threat intelligence and leverage this information to improve internal detection and defense mechanisms. As the InfoSec Institute points out, the SOC consumes data from within the organization and correlates it with information from a number of external sources that deliver insight into threats and vulnerabilities. This external cyber intelligence includes news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts that aid the SOC in keeping up with evolving cyber threats (already discussed in some detail above). SOC staff must constantly feed threat intelligence into SOC monitoring tools to keep up to date with threats, and the SOC must have processes in place to discriminate between real threats and non-threats.

Truly successful SOCs utilize security automation to become effective and efficient. By combining highly-skilled security analysts with security automation, organizations increase their analytics power to enhance security measures and better defend against data breaches and cyber attacks. Many organizations that don't have the in-house resources to accomplish this turn to managed security service providers that offer SOC services.

[22] Visit http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/, to download the latest version of the report. Site viewed 06 March 2017.

A great reference for those seeking to understand how to build, operate and maintain a world class SOC, or become familiar with the characteristics of one if a decision is made to outsource the capability is the book *Security Operations Center: Building, Operating and Maintaining Your SOC* by Joseph Muniz, Gary McIntyre and Anthem Aladdin, published by Cisco Press in 2016. This book can serve as a quasi-definitive reference source for anyone tasked with learning about, funding, or building and operating a SOC.[23]

7.9 Managed Security Services Provider (MSSP)

According to Gartner, a **managed security service provider (MSSP)** provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. MSSPs use high-availability security operation centers (either from their own facilities or from other data center providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.[24] An MSSP is usually an Internet service provider (ISP) that provides an organization with some amount of network security management, which may include virus blocking, spam blocking, intrusion detection, firewalls, and virtual private network (VPN) management, as mentioned above. An MSSP can also handle system changes, modifications, and upgrades. MSSPs have evolved in various ways. Some traditional ISPs, noting the increasing demand for Internet security that has occurred in recent years, have added managed security to their repertoires. A few security vendors have added Internet access, thus becoming MSSPs. Still other MSSPs have come into existence as brand new entities.

An MSSP offers cost savings by allowing an organization to outsource its security functions. But some organizations are reluctant to give up complete control over the security of their systems. In addition, there may be considerable variability in competence among MSSPs.[25] The TFOPA-defined EC3 concept discussed above is a variant of the MSSP concept. Given the general lack of security expertise and capability at PSAPs and in public safety organizations globally, looking at MSSPs to perform this function for European PSAPs and control rooms is strongly recommended, as the cost to hire and stand up internal security functions that can deal with the exploding number of security threats will be prohibitive for all but the largest and most well-funded centers.

8 Policy and Operational Aspects of Cybersecurity

Having spent a fair amount of "ink" discussing the various technologies and systems used to monitor and control information systems security, it is important to note that overall security is not only a technology problem, but is a SYSTEMS issue that involves putting in place good policies, hiring the right people, and establishing efficient operational procedures, as well deploying the latest technology. In fact, many commentators have said that security is more of a PEOPLE issue than a technology one. Policies and procedures that encourage proper, security-aware behavior on the part of internal staff can go farther than the best technology system, since people are many times the biggest security risk in the system. Above all, an integrated system of policy, controls, and operational procedures should help with developing as set of cybersecurity controls that, above all, should

- Accurately identify and authenticate all entities seeking access to a system
- Authorize access to only those objects that the entity's level of trust permits
- Monitor and control activities during the time that the entity is granted access
- Ensure against unauthorized access, or manipulation of data
- Ensure against unauthorized manipulation of system objects

Part of the trouble with building cybersecurity programs and systems that insure operational security in the Internet era is due to the fact that "cybersecurity" is at best an ill-defined field. Since there is no clear definition of the field, the profession, and the actual protection of computers and information tends to be

[23] Muniz, Joseph, Gary McIntyre and Nadhem AlFardan. *Security Operations Center: Building, Operating, and Maintaining Your SOC*. Indianapolis, IN: Cisco Press, 2016/
[24] See http://www.gartner.com/it-glossary/mssp-managed-security-service-provider/, viewed 06 March 2017.
[25] Taken from http://searchitchannel.techtarget.com/definition/MSSP, viewed 06 March 2017.

characterized by a long track record of hit-and-miss failures. This confusion about what is cybersecurity beyond the technical elements usually associated with the field stems from the fact that it could potentially comprise concepts from a number of disciplines. Some content from each of the following fields could reasonably seen to fall within the boundaries of "cybersecurity:"

- Business management, contributing such concepts like security policy and procedures and regulatory compliance
- Traditional technical studies of computer security
- Knowledge of the field of networking adds essential recommendations about how to protect data in transit
- Software engineering add the necessary system and software assurance considerations like configuration management and lifecycle process management
- Law and law enforcement contribute important ideas about such topics as intellectual property rights, privacy and cyber law, legislation and litigation and prosecution of computer crimes
- Behavioral studies address essential human factors like discipline, motivation, training and certification
- Ethics, with its consideration of the personal and societal implications of information use and protection also plays a role here

To achieve true comprehensive cybersecurity protections, principles and methods from each area must be integrated into a complete and cohesive program and body of knowledge. Strong, coordinated governance and control programs must be in place to make any deployed security technology effective and cost efficient. An evaluation must be made of potential assets that might be targets for compromise. These include organization assets such as:

- Hardware and system assets
- Software applications
- Facilities
- Personnel (e.g., the human resource investment)
- Information data / assets
- Organizational Interfaces (e.g. business relationships)
- Organizational agreements (e.g. plans, contracts)

The list of areas under threat that might require some form or control or countermeasure against breach or theft is a long one; if nothing else, this list should convince public safety personnel reading this document that a comprehensive security plan for insuring safe and uncompromised operation of NG112 systems involves MUCH than buying and installing a few firewalls. That list includes the following:

1. Policy
2. Governance control
3. Personnel security
4. Physical and environmental security
5. Asset management
6. Access control
7. Security of operations
8. Network security
9. Computer security

10. Software development and maintenance security
11. Acquisition
12. Incident management
13. Compliance
14. Continuity
15. Elements of human factors such as training and education

This list can be considered a summary of the potential threat vectors in any cybersecurity control situation. Any or all of these areas must have effective countermeasures in place in order to protect against the types of threats that be identified in each category. To do this, the organization must first undertake a comprehensive analysis of the threat environment that exists. The need for this a priori threat assessment was discussed earlier in this paper and its importance cannot be stressed enough. It should be clear from this brief analysis of the "non technical" parts of good security plan development and execution that sufficient time must be devoted to developing the policy, plan, and procedure parts of an organizations security approach, long before any decisions on what types of technology should be deployed. Failure to do this up front will result in needless problems down the line. It is strongly recommended that organizations that lack the skills and resources of specialist organizations, either public or private, that can help with setting up a comprehensive and efficient security plan.[26]

9 Data Security and Privacy Issues in Public Safety

Amidst the talk of insuring cybersecurity is as tight as it can be to insure the rollout of NG112 goes smoothly, there is another, related issue and this has to do with data privacy. Data privacy regimes for public safety differ markedly across the globe but all have to do with how PII is handled when members of the public reach out to emergency services to request help and assistance. In the USA, from the start of the use of the 9-1-1 systems in the 1960's, it has operated under a legal regime of "implied consent," i.e., the very act of dialing 9-1-1 "implied" the caller's consent to have their name, callback number and address shared with PSAPs and first responders. US states backed this "consent" up with liability waiver laws that provided telephone providers, database providers, PSAPs and first responders with "immunity" from prosecution related to data and procedures associated with emergency response. These legal protections were extended by various Federal laws to wireless and VoIP carriers and "alternative emergency services providers." To this day, many US jurisdictions allow the public release of 9-1-1 call recordings to the press and public. In other parts of the world, notably Europe but also Japan laws concerning the governance of the release of PII have been tighter, but regardless of jurisdiction, under older technological regimes, the public, and public safety authorities have only had to worry about protecting as small set of data (name, address, and telephone number) and recordings of voice calls. In the NG era, this is no longer the case.

The introduction of NG112 across Europe will result in a system that will, at least theoretically, allow the public to not only "call" 112, but also share text, image and video data with call takers and first responders. The potential for "leakage" of PIIgoes up EXPONENTIALLY with the rollout of NG112. All of the methods, procedures, and technologies discussed elsewhere in this document take on a new significance and urgency given the sheer volumes of data, much of it potentially PII, that will be "sloshing around" the NG emergency response system.

It should be clear this discussion that serious consideration of data security and privacy will be key in the new world of.

10 Designing and Operating Cybersecurity and Privacy Protection: Some Considerations.

An important design consideration in NG112 is the principal that there is "No Security in Obscurity". This concept means that we must have active, effective secure mechanisms that prevent unauthorized access, and we do not depend on hiding access, or making resources hard to find. Attempting to achieve security through obscurity is actually quite common, but has been repeatedly shown to be ineffective as the only measure. The security issues we face arise through deliberate attempts to manipulate systems, not accidental mishaps. The level of sophistication of attackers is very high, and none of the obscurity mechanisms work against sophisticated attackers. If we can stop sophisticated attacks, we can also stop unsophisticated attackers. We put a lock on the safe, not hide it from view. Considerations in this document have purposely departed from the concept of "Security by Obscurity" and rely on active protection.

[26] This discussion is taken from Kohnke, Anne, Dan Shoemaker, and Ken Sigler. *The Complete Guide to Cybersecurity Risks and Controls*. Boca Raton, FL: CRC Press, 2016. PP. 5-6, 17, and 36.

Another important design consideration is to avoid relying on "walled gardens". Walled gardens refer to attempts to build secure boundaries limiting access to a network, and then assume that whatever is inside the network is safe. Creating secure borders to networks is certainly a primary defense mechanism and is highly encouraged. However, it has proven nearly impossible to maintain the borders securely, and thus such borders are regularly breached, not only by intruders, but by well-meaning insiders trying to get their job done. The need to well defend the interior of the NG112 Core System (NGCS) at all layers is further necessitated by successful attacks which can manage to breach one system from the outside, and use that breach to exploit vulnerabilities of other systems from the inside. Thus the inside of the NGCS should be treated as if it was the open Internet, and all activities within it should be protected. Current NG112 standards require all external interfaces on all functional elements use secure protocols, and make use of uniform identity, authentication, authorization, privacy, integrity and non-repudiation mechanisms. Even systems beyond the purview NG112 standards should employ similar security mechanisms to protect them from harm.

Given the fact that the "walled garden" approach to security is no longer tenable, a better approach for good design today is a "defense in depth" strategy. Defense in depth is a strategy common to both military maneuvers and information security. In both senses, the basic concept of defense in depth is to formulate a multilayered defense that will enable achievement of a successful defense should one or more of defensive measures fail. Figure 4 is an example of the layers to put in place to defend assets from a logical perspective; at the very least, defenses at the external network, internal network, host, application, and data levels are necessary. Well-implemented defenses at each layer will make it very difficult to successfully penetrate deeply into a network and attack assets directly.

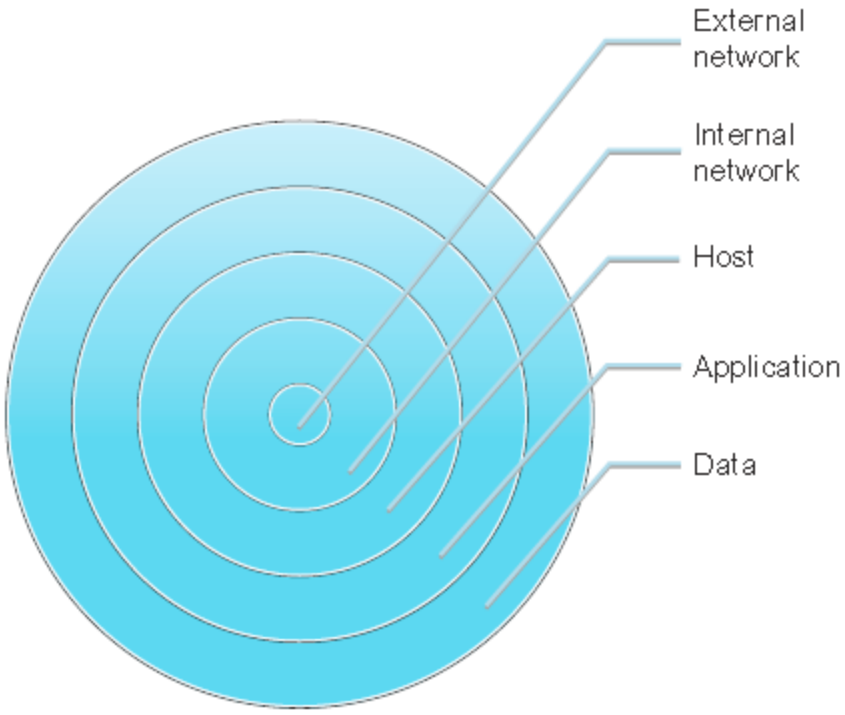


Figure 4: Defense in Depth

When we look at the layers that might be present in a defense in depth strategy, we will likely find that they vary given the particular situation and environment we are defending. As discussed, from a strictly logical information security perspective, we would want to look at the external network, network perimeter, internal network, host, application, and data layers as areas to place our defenses. As we can see in Figure 5, some of the defenses we might use for each of the layers we discussed are listed. In some cases, we see a defensive measure listed in multiple layers, as it applies in more than one area.

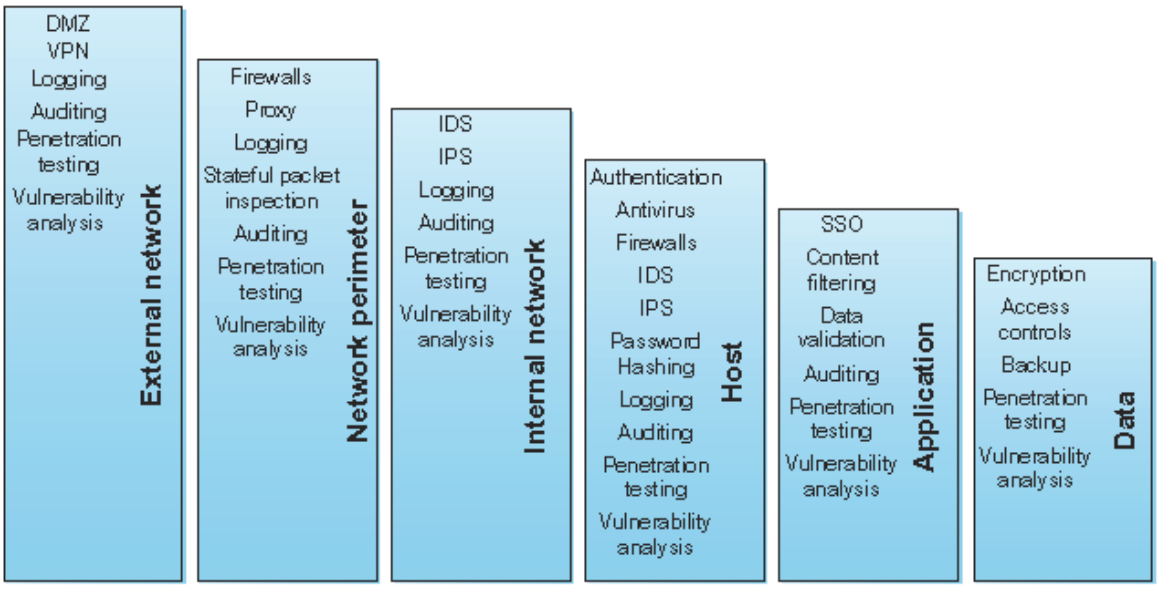


Figure 6: Defenses in Each Layer

Defense in depth is a particularly important concept in the world of information security. To build defensive measures using this concept, you put in place multiple layers of defense, each giving an additional layer of protection. The idea behind defense in depth is not to keep an attacker out permanently but to delay him long enough to alert us to the attack and to allow us to mount a more active defense.

11 Security and Privacy issues in the NG112 Architecture

With regard to the Emergency Services IP Network (ESInet), it must include a firewall solution that provides security and protection to the system. All interfaces connected to the ESInet should be in accordance with mandated security requirements:

- Secure remote access must be strictly controlled. Control must be enforced via remote access authentication using security tokens that provide one-time password authentication or public/ private keys with strong pass-phrases.
- The security solution must include a method to control access to network resources to prevent sabotage and the compromise (intentional or unintentional) of sensitive information.
- Remote Access control should be enforced via network and system level auditing.

To this end, the firewall component of the Border Control Function (BCF) inspects all traffic transiting the network edge. It provides both application and network layer protection and scanning. In the application layer, the BCF scans and eliminates known malware attacks from extranet and intranet sources at OSI layer 7 before they ever reach a user's workstation or a production server or another end point located inside the ESInet. These act as the primary layer of defense for most malware attacks that are protocol specific. Network layer protection is provided by access control through the use of access control lists and port-based permission/denial management. The network firewall also mitigates lower layer protocol attacks. In addition, the BCF provides Denial of Service (DOS) and Distributed Denial of Service (DDOS) detection and protection.

The primary functions of the Session Border Control (SBC) element of the BCF include, but are not limited to Identification of emergency call/sessions and priority handling for the IP flows of emergency call/session traffic; forwarding of emergency call/sessions to an Emergency Service Routing Proxy, the first Core Service element inside the ESInet; Adding Call and Incident Tracking identifiers to the signaling and adding the Resource-Priority header if not already included; protection against SIP-specific and general DDoS attacks; other functions as specified in the EENA NG112 Long Term Definition document referred to earlier in this paper.

ESInet providers should also be required to provide anti-virus software on all devices that allow ingress and egress to the ESInet. The anti-virus software must be designed to support safe and secure interconnection all

PSAPs and end sites across the network. The anti-virus software deployed should use an antivirus database that scans incoming and outgoing packets for the presence of malicious software, and blocks and logs such activities. The anti-virus database should also be maintained and coordinated through to minimize the potential of multiple databases on the same network.

Specifically, virus and malware protection should be provided on all ESInet components and on the access points to the NGCS, extending to the demarcation point at the PSAP. The most current virus and malware definitions must be provided and updated on a continuing basis.

12 Conclusion and Recommendations

In an all IP-world, providing for cybersecurity and data privacy are key issues that were not as paramount in the old system. As mentioned many times in the text, while moving to IP-based communications systems provides new capabilities, and enables new possibilities for better public safety, it will require new vigilance, as well as the deployment of news systems and processes, to insure security and privacy are protected and provided. Of necessity, this paper can only introduce the main topics that will be of concern to public safety managers and professionals in the future; there is so much more that can, and should, be said, and the need for sound cybersecurity systems and procedures design will be paramount in the future.

Some of the conclusions and recommendations that can be drawn from the discussion in this paper include:

- The ultimate success of NG112 will in large part depend upon the successful implementation of cybersecurity and data privacy protection, rules, policies, procedures and technologies. The new capabilities and possibilities that are created due to the inherently open nature of the new system can be threatened by inadequate security and data protection mechanisms.

- Emergency services should be designated as critical infrastructure in all jurisdictions, to indicate that it is as essential to the working of a modern industrial society as the other key sectors like transportation and power utilities.

- Adequate cybersecurity and privacy protection in the era of IP-based systems involves more than deploying security systems technology like firewalls and intrusion detection systems. Policy, operational procedures, threat intelligence and assessment and information sharing mechanisms with friendly stakeholders must all be put in place

- Employing a standard and generally accepted Information Security Model (ISM) and risk management framework is key to mapping out security vulnerabilities and doing a risk assessment around the ones identified.

- Documented incident response plans will be essential to successfully combating the security incidents that are sure to arise once migration to the new system has taken place.

- Security is not only a technology problem, but as SYSTEMS issue that involves putting in place good policies, hiring the right people, and establishing efficient operational procedures, as well as deploying the latest technology.

- Strong, coordinated governance and control programs must be put into place to make any deployed security technology effective and cost-efficient.

- Given the sophistication of today's hackers and others intent on compromising the security of information and communications systems, a "walled garden" approach to security will not work and a "defense in depth" approach will work much better.

ANNEX: Defining and Protecting Critical Infrastructures: The Case of Public Safety in the US

Other global governmental jurisdictions, most notably the United States, have declared public safety infrastructure, including citizen-to-authority emergency communications such as 9-1-1 in the US, the equivalent of 112 service in Europe, to be "critical infrastructure" and therefore worthy of special attention and focus when it comes to cybersecurity efforts. Today, the USA has 16 specifically identified categories of "critical infrastructure." Emergency services are one of those 16 enumerated categories. They are identified in Presidential Policy Directive-21 (PPD-21), dated 12 February, 2013. The US Department of Homeland Security (DHS) is the designated "Sector Specific Agency (SSA)" responsible for overseeing cybersecurity and other protection efforts for the emergency services sector. Emergency services have been considered critical infrastructure in the US since 1996 an directives issued at that time by the Clinton Administration. This designation puts emergency services like 9-1-1 (and by extension, 112) on par in terms of importance with such services as telecommunications networks, electric utilities and transportation and water systems.[27]

Designation of emergency services as critical infrastructure indicates that it is as essential to the working of a modern industrial society as the other capabilities mentioned above. It is important, however, as well to note that despite this designation, public safety continues to be endemically underfunded in the US and that this designation alone has not been enough to insure the timely rollout of NG9-1-1 capabilities in the US. Concerted efforts on the policy, regulatory and funding issues, are required to insure rollout of the system, AND necessary cybersecurity protections, in any jurisdiction.

The US DHS has adopted the Threat Agent Risk Assessment methodology, developed by Intel to measure current cybersecurity threat risks. It is used to identify the most likely threat risks and pre-establish, as much as possible, known areas of exposure across critical infrastructure areas. This data is used by the various sectors to help align control resources applied and the most likely threats to be encountered, so limited resources are not wasted in a vain attempt to "protect against everything." The US Federal government also has established a host of different cybersecurity threat information sharing programs and other Information Sharing Environments (ISEs) dedicated to helping public and private sector entities share cybersecurity threat and incident information that will benefit all players. Many of these are sector specific and encourage the gathering of parties in individual industry sectors into so-called Information Sharing and Analysis Centers (ISACs), setup specifically to encourage cybersecurity information sharing in a particular industry sector.

DHS is not the only actor in the space, and other US Federal entities, particularly the National Institute of Standards and Technology (NIST) and the Federal Communications Commission (FCC) have been especially active in providing 9-1-1 PSAPs (equivalent organizations to 112 Control Rooms in Europe) with tools and documentation that should prove effective in assisting with NG112 cybersecurity as well. Of particular note and value to creating cybersecurity policies, programs and solutions procurement guidance is the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, first issued on 12 February 2014. This framework enables organizations, regardless of size or degree of cybersecurity risk, to apply core elements of the framework to improve their overall cybersecurity posture. These five (5) core elements of the framework are:

- ***Identify*** – Develop the organization understanding to manage cybersecurity risks to systems, assets, data, and capabilities.
- ***Protect*** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services, like 9-1-1 or 112 services. The Protection function supports the ability to limit or contain the impact of a potential cybersecurity event.
- ***Detect*** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events.
- ***Respond*** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond function supports the ability to contain the impact of a potential cybersecurity event.

[27] Details in this discussion taken from Johnson, *Op. Cit.*, pp. 34-40.

- ***Recover*** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.

These five functions are used to organize basic cybersecurity activities at their most critical levels. The Framework provides a structure that both advises and guides the management of risk while providing an assessment strategy to address and manage cybersecurity threats and incidents. NIST was directed to create this framework by Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, issued by President Obama on 12 February 2013. The Framework 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*** [emphasis added], or any combination of those matters." The Cybersecurity Framework provides a very structured and organized methodology for organizations to:

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improvement
- Assess Progress towards the target state, and
- Communicate with stakeholders about the cybersecurity risk

More specifically the Framework is composed of three (3) components:

The Framework Core – The Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core consists of the five concurrent and continuous functions outlined above, which, when considered together, provide a high-level strategic view of the lifecycle of an organization's management of cybersecurity risk.

Framework Implementation Tiers – Provide context on how organizations view cybersecurity risk and the processes put in place to manage that risk. The Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework.

Framework Profiles – Represent the outcomes based on business needs that an organization has selected from the Framework categories and subcategories. The Profiles can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.[28]

As should be apparent from a comparison of the earlier discussion about incident response and the characteristics of the Cybersecurity Framework, it is based upon current industry best practices and while likely not 100% applicable to all possible European scenarios, it should nevertheless be used as one of the main reference documents for developing NG112 cybersecurity processes and procedures, as it is being used to do this for NG9-1-1 in the USA. Given the fact that NG9-1-1 and NG112 share the same technology base, use of the NIST Cybersecurity Framework for NG112 is eminently reasonable.

The FCC, as mentioned, has also been very active in this space, providing resources geared to the use of NG9-1-1 in the USA that should also be quite relevant an useful for 112 Centers as well. In 2015 and 2016, the FCC chartered the so-called "Task Force on Optimal PSAP Architecture," most often shortened to "TFOPA." TFOPA created three (3) different working groups, each focused on a different area of importance to PSAPs, to help it craft a set of documents containing the Task Force recommendations. The three working groups focused on Optimal Cybersecurity For PSAPs (WG1), Optimal NG9-1-1 Architecture Implementation (WG2), and Optimal Resource Allocation ("Funding") (WG3).

The work of TFOPA WG1 is of particular relevance here. Each TFOPA WG produced a final report at the end of 2015 and a supplemental report at the end of 2016. These documents can be found at the FCC's TFOPA

[28] Discussion of NIST Framework based upon Johnson, *Op. Cit.*, pp. 28, 58-63.

website[29]. The documents of WG1 are highly recommended sources for helping public safety official and managers get a better grasp on the aspects of cybersecurity if interest to PSAP managers and their overseeing public officials. While they were developed with US NG9-1-1 in mind, they are also applicable to NG112.

In particular, the TFOPA WG1 activity defined a concept known as the ***Emergency Communications Cybersecurity Center*** or EC3 concept, which is adaptable from the world of NG9-1-1 to NG112 and therefore is of real relevance to the rollout of NG112 services. The EC3 is described thus in the WG1 final report: "The intent of [adding this EC3 concept to the]…this logical architecture recommendation is to create a centralized function, and location, for securing NG networks and systems. By centralizing certain features, including cybersecurity in general, and intrusion detection and prevention services (IDPS) specifically, public safety can take advantage of economies of scale, multiple resources, and systems and best practices which may already be in place or at a minimum readily available for deployment and use."[30] The EC3 concept is illustrated in Figure 3:

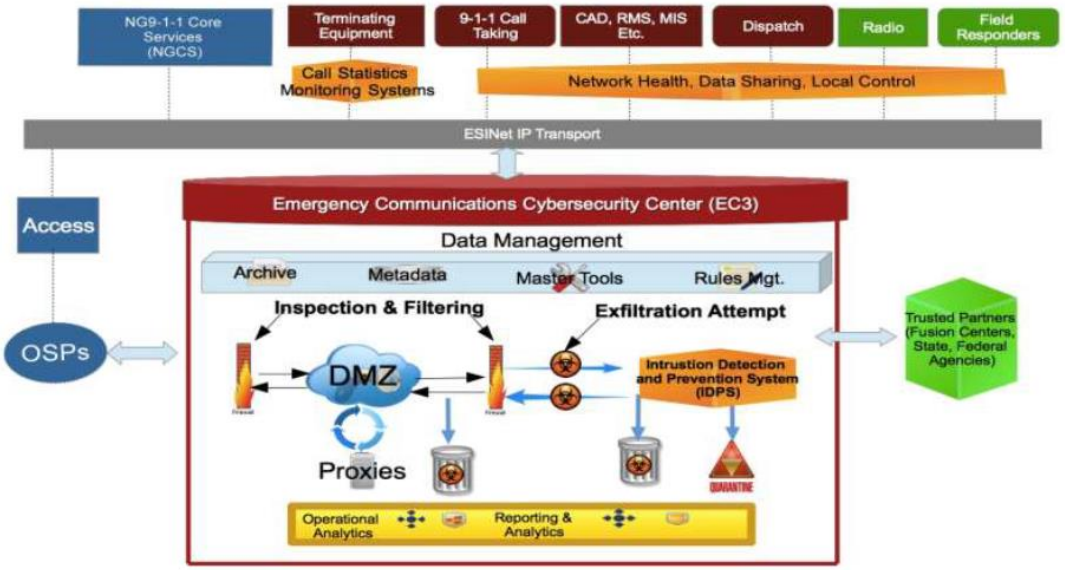


Figure 3: Proposed Architecture for Emergency Communications Cybersecurity Center (EC3)[31]

The EC3 is a managed security service, like a regional Security Operations Center (SOC) that provides essential security services to PSAPs. Though Europe may not have the "numbers problem" the US has in terms of sheer number of PSAPs to be protected, the same lack of true local cybersecurity expertise and technology DOES exist and a modified version of the EC3 concept could be implemented in Europe. The WG1 documentation contains other recommendations that are well the perusal of European public safety authorities.

One other, very recent, FCC activity of note and relevance to NG112 Cybersecurity is the publication of an FCC whitepaper entitled *Cybersecurity Risk Reduction*, published 18 January 2017 and authored by the outgoing Chief of the FCC Public Safety and Homeland Security Bureau, RAdm. David Simpson, USN (Ret.). The intent of this document is as follows: "This white paper describes the risk reduction portfolio of the current Commission and suggests actions that would continue to affirmatively reduce cyber risk in a manner that incents competition, protects consumers, and reduces significant national security risks." It has a section dedicated to cybersecurity in public safety. While much of the document is focused on policy recommendations for the FCC (which might be of use to equivalent national regulatory authorities in the EU territories) the report has this to say about NG9-1-1 cybersecurity (and therefore by extension, NG112):

[29] https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point
[30] Taken from TFOPA WG1 *Final Report*, p. 32.
[31] Taken from TFOPA WG1 *Final Report*, p. 36.

> "Next-generation 9-1-1 (NG9-1-1) systems, which rely on IP-based protocols and services, will allow responders to take advantage of capabilities such as text and video messaging. Public safety answering points (PSAPs) will be able to route calls and provide alternative routing to ensure resiliency during an emergency or disaster. However, in spite of these important benefits, cybersecurity challenges increase when PSAPs are connected to multiple devices and networks that make use of the Internet protocol...More modern IP-based 911 service changes service demarcation boundaries and the enhanced processing for call handling, dispatch, and records management has expanded the 911 attack surface. Many jurisdictions have not yet organized their cybersecurity programs..."

This discussion, along with the document's Appendix B, "The Market for ISP Cybersecurity" should be required reading by European public safety authorities looking for policy guidance analogues to help guide European policy setting in this all-important area.[32]

It should be clear from this brief overview of protection measures being taken in other jurisdictions with regard to "critical infrastructure" such as systems equivalent to NG112 systems, Europe, too, should use means at the disposal of individual countries and the European Commission to designate NG112 "critical infrastructure" and work to codify and promulgate, rules, regulations, and recommendations optimized to protect this resource that will be so critical to the citizens of the European Union.

References

[1] Andress, Jason. ***The Basics of Information Security, Second Edition***. Waltham, MA: Syngress / Elsevier, 2014.

[2] Bellovin, Steven M. ***Thinking Security: Stopping Next Year's Hackers***. New York: Addison-Wesley, 2016.

[3] Dalziel, Henry. ***How to Define and Build an Effective Cyber Threat Intelligence Capability***. Waltham, MA: Syngress / Elsevier, 2015.

[4] Goodman, Marc. ***Future Crimes: Inside the Digital Underground and the Battle for Our Connected World***. New York: Anchor / Penguin Random House LLC, 2016.

[5] .Johnson, Thomas A., Ed. ***Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare***. Boca Raton, FL: CRC Press, 2015.

[6] . Kaplan, James M., Tucker Bailey, Derek O'Halloran, Alan Marcus, and Chris Rezek. ***Beyond Cybersecurity: Protecting Your Digital Business***. Hoboken, NJ: John Wiley & Sons, 2015.

[7] . Kohnke, Anne, Dan Shoemaker, and Ken Sigler. ***The Complete Guide to Cybersecurity Risks and Controls***. Boca Raton, FL: CRC Press, 2016.

[8] . Muniz, Joseph, Gar McIntyre, and Nadhem AlFardan. ***Security Operations Center: Building, Operating and Maintaining your SOC***. Indianapolis, IN: Cisco Press, 2016.

[32] Discussion based on Simpson, *Cybersecurity Risk Reduction*, Washington, DC: Federal Communications Commission, 18 January 2017, pp. 20-22. (https://www.fcc.gov/document/fcc-white-paper-cybersecurity-risk-reduction)