EENA Document

Cybersecurity

Guidelines and Best Practices for Emergency Services

european emergency number association

This document was written by members of the EENA Working Group on Cybersecurity. This WG was open to EENA members and non-members .

Authors: **Pablo GUTIERREZ ASTILLEROS** (Telefónica, EENA Technical Committee Vice-chair) and **William MERTKA** (ServerCentral, EENA Technical Committee Vice-chair).

Contributors: **Hadi EL-KHOURY** (Information Systems Security Association (ISSA) French Chapter, France), **Markus BORNHEIM** (Ayava, Germany), **Bernard BRABANT** (Agence municipale de financement et développement des centres d'urgence 9-1-1 du Québec, Canada), **Blair HANKINS** (Independent Cybersecurity Expert, USA), **Alan HEWARD** (Ministry of Business, Innovation & Employment, New Zealand), **Min HUANG** (Huawei, China), **Wolfgang KAMPICHLER** (Frequentis, Austria), **Dan LAZAREAN** (Smartfactor, Romania), **Cristina LUMBRERAS** (EENA), **Christine RUNNEGAR** (Internet Society (ISOC)), **Henning SCHMIDTPOTT** (Integrated Control Centre – Freiburg, Germany) and **Kirsty THOM** (PeoplePager, New Zealand).

DOCUMENT DETAILS

Version: 1.0

Revision date: 15-06-2018

CONTENTS

Timely security is more critical than ever...

1. Executive Summary

This paper aims to increase awareness among Public Safety organisations about the impacts related to cyber vulnerabilities, risks and threats and provides some recommendations for mitigation.

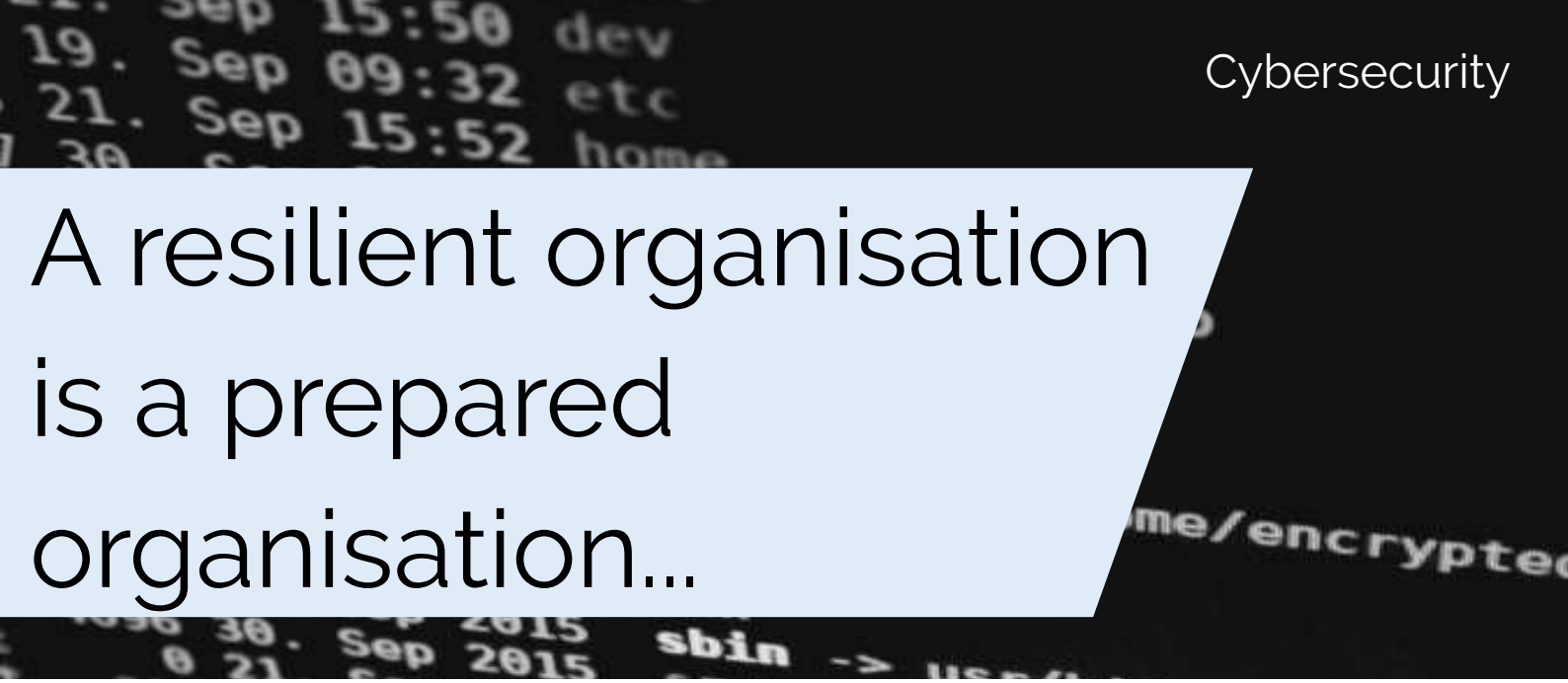
Cybersecurity, for the purposes of this document, refers to the technologies, processes and practices designed to protect users, networks, computers, programs and data from attack, damage or unauthorised access. Ensuring the cybersecurity of Public Safety systems requires coordinated efforts throughout an entire organisation and its peers.

One of the most problematic elements of cybersecurity is the quick and constant evolving nature of security threats. Cybercriminals are rapidly evolving and adapting their hacking techniques and hacking tools are increasingly available for purchase, making it easier for anyone to launch an attack. They attack quickly, making timely security more critical than ever. Consequently, one of the first actions involved in initiating an effective cybersecurity strategy is to gain an understanding of the cyber risk landscape.

Public Safety organisations, and more concretely, Public Safety Answering Points (PSAPs), have recently suffered cyberattacks. Protecting their information technology infrastructure and information involves the development and implementation of appropriate and effective safeguards to ensure delivery of critical Public Safety infrastructure services.

The main recommendations are:

- Incorporate cybersecurity as part of the general risk assessment of the organisation
- Include cybersecurity strategies in procedures and policies
- Assign employees responsible for cybersecurity in the organisation
- Train all employees with digital access on security policies and procedures.
- Assess and implement technological solutions, using 3rd party specialists, if needed.
- Perform cybersecurity audits and infrastructure vulnerability tests
- Perform cyberincident exercises



A resilient organisation is a prepared organisation...

2. Introduction

For the purposes of this document, cybersecurity means the strategies, processes, practices and measures for managing security risks to Public Safety digital services and their underlying infrastructure and systems.

A good definition 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."*[1]

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."*[2] Influence refers to cybersecurity staff having to "influence" others in the organisation 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 the fact that comprehensive cybersecurity depends not only on technical means, but also on policies, procedures, and above all PEOPLE. Poorly trained staff is one of the main reasons for cybersecurity breaches. Thus, the need for vigilance, training, and programs geared toward "upping the cybersecurity quotient" of everyone involved with the public safety service delivery chain.

Technology currently used by emergency services can be attacked. An EENA Technical document describes the "Security and Privacy Issues in NG112"[3], but this Guidelines and Best Practices document emphasizes the fact that attacks can occur today.

Currently, there are more machines behind IP addresses than humans. As Internet of Things (IoT) becomes pervasive, the threat of cyberattacks taking out mission-critical infrastructure like power grids to telecommunications networks is increasingly real. This can affect anything and everything from connected cars to hospitals to airplanes.

To avoid a catastrophe, organisations need to have cybersecurity solutions in place and thorough knowledge about the different kinds of cyberattacks that can occur. A resilient organisation is a prepared organisation.

[1]Kaplan, James M, et. al. *Beyond Cybersecurity: Protecting Your Digital Business*. NY, John Wiley and Sons, 2015. PP. xiv – xv.

[2]*Ibid*.

[3]http://eena.org/download.asp?item_id=234

What are the aims of cyberattackers?

3. Examples of cyberattacks

A cyberattack is an attack initiated from a computer or other Internet-connected device (e.g. consumer IoT) against a computer system or individual computer that compromises the confidentiality, integrity or availability of the computer or information stored on it.

Their objectives include:

- Gaining, or attempting to gain, unauthorized access to a computer system or its information.
- Unwanted disruption or denial of service attacks, including the take down of entire web sites or other Internet services.
- Installation of viruses or malware - that is malicious code on a computer system which may spread rapidly to other computers on the internal network.
- Unauthorized use of a computer system for processing or storing information (e.g. cryptojacking).
- Preventing access to systems and/or data.
- Changes to the characteristics of a computer system's hardware, firmware or software without the owner's knowledge, instruction or consent
- Stealing information
- Inappropriate use of computer systems by employees or former employees or contractors.
- Tampering the data or injecting fraud data into the system
- Erasing the footprints of the attack activities and denying the operations

Some of the forms cyberattacks can take are listed below, but stakeholders need to use their "imagination" to think about other possible types of attacks. Some of them may not seem to directly affect the emergency services operations, but, depending on the type of architecture employed by the PSAP (e.g. shared servers) they may have an impact.

How to identify a fake communication?

Phishing

Phishing scams are appropriately named. Phishing can occur via different means, e.g. through social media, a messaging application, VoIP, SMS, a telephone call, email, etc. We will take the email as an example. Simply put, they are email scams that try to lure people into clicking on links that have viruses, much like someone trying to lure fish with bait. The phishing communication will generally offer something lucrative and tempting. It will likely disguise a link to a familiar site, in order to get someone to click or download malicious software. The links are often used to steal login credentials.

Phishing scams are gaining in popularity. There is no question that everyone is at risk these days. As a result, it is very important to know how to identify a fake communication without falling prey to its bait.

Most of the time, phishing emails are quite sophisticated and look very authentic and legitimate. Here are some examples:

- A sense of urgency: “Hurry,” “ASAP,” “need this done by…”
- A threat: “We will suspend your account”
- Directions to do something: “Validate,” “‘verify,” “confirm,” “update”
- Requests for personal information: SSN, address, account information, and login credentials
- Unknown web addresses: These may be doctored to look legitimate

Some of the common indicators that a phishing communication is not authentic are:

- Fake/poor quality images
- Poor spelling/grammar
- Improbable scenarios

Best practices to spot phishing emails are...

There are three main attack vectors employed in Phishing communications:

- Attachments that look like valid documents. Common are bogus financial invoices or delivery service notifications
- Links that appear to be legitimate but link to a site with malicious software
- Credential or information theft. Very common and has the user follow a link that will harvest user logins or other key information.

Phishing emails usually have something spelled wrong or seem "phishy," and usually target large volumes of people. There are also newer, more precise, methods of targeting, called spear phishing. Like phishing emails, spear phishing attacks pretend to be a trusted source. While phishing emails target many people, spear phishing attacks usually target only a few specific people or departments that have been researched beforehand. Spear phishing attacks are much more successful because the perpetrators have done the research and customized the email, and it can be harder to identify as fake. In general, spear phishing is targeted at a particular group within an organisation that has valuable and confidential information – for example finance or human resources departments. There are also many targeted examples of phishing that focus on executives, e.g. CEOs, CFOs, and other high-level decision-makers.

Best practices for authentication of email are the use S/MIME or PGP to sign emails.

Best practices to distinguish phishing emails are:

- Ask yourself: Was the email expected? Do I know the sender? Is the request in the email normal?
- Hover your cursor over the link…Is it legitimate? Look at it closely! This is usually simple to do. The sender will include some content in the URL that matches your expectation, but the domain name will not be something you expect.
- If the email is from someone claiming to be a person you know, call (or use some other out of band communication tool to contact) that person to verify if they sent the email.
- Another way to verify email source is recognise that the "envelope-from" sender address could be easily spoofed. If the email program has a way to inspect the "reply-to" address the user could verify the identity of the sender.

Ransomware

In the cyberworld, ransomware is a constantly evolving and growing threat. Ransomware is a form of malware software that "kidnaps" access to your network, applications, or information until a certain amount of money is paid by the victim.

Ransomware exploits the slow pace of security patching, systems that are dependent on old software, and poor backup practices. It also provides a smokescreen for other acts including stealing data and credentials, or even deleting data.

It does this by encrypting certain information, so you cannot get to the information, or blocks access to systems and applications. Ransomware usually infects your computer or device with a Trojan virus from phishing emails or malicious programs on a website. Once it is installed, a ransom message usually pops up when the user restarts their device. Ransomware attacks are increasingly popular among attackers, as they have primarily shifted away from attacks on servers and on to attacks focusing on endpoints. In general, endpoint users are typically less technical, and are sometimes are using legacy equipment that cannot be easily patched and have different levels of trust.

The impact of ransomware can be devastating. You can permanently lose important and private information, you can expose critical flaws in your organisation, impact your reputation, and potentially lose a lot of money. However, even if you pay the ransom, it does not guarantee that you will get the information back.

Naturally, following good backup procedures for your information will mitigate the impact of such an attack on an end user machine. Public Safety organisations should ensure they have at least two backups (one stored remotely), and they should regularly test that they are able to quickly restore their systems from backups. They should ensure devices and systems are patched, their critical services should have built-in redundancy, they should be alert to new threats (e.g. by following Computer Security Incident Response Team (CSIRT) notices) and make sure users are alert to phishing and other types of social engineering.

DDoS

Distributed Denial of Service (DDoS) attacks use already infected systems or a group of malicious actors to target one website by flooding it with traffic, generating so many HTTP or HTTPs request responses and that it is rendered inaccessible. These attacks come from many different sources, which makes them extremely difficult to stop, since these attacks originate from so many different addresses.

Popular websites, such as Netflix, the *New York Times*, and Reddit have all been susceptible to DDoS attacks in the past.

Attacks come from many different sources, making them extremely difficult to stop...

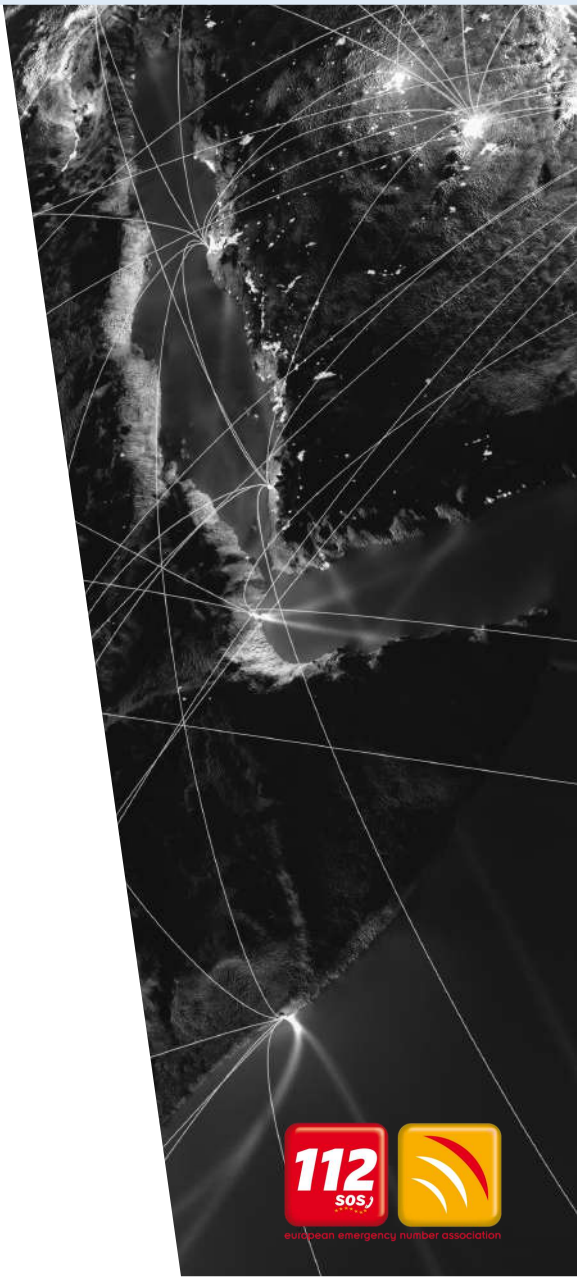
Spam

Spam emails are emails that are often anonymous, sent to large groups of people, and unsolicited. Most email inboxes have a spam filter, so you usually won't see spam emails unless you go into your spam folder. However, there are many spam emails that get past the spam filter and appear in your inbox, unscathed. These spam emails get past the spam filter in many ways. One common way for the spammer to succeed is to continually setup new servers with new IP addresses to get past the IP reputation filter.

It is worth mentioning that Spam is not limited to email – it has spread to all forms of electronic communication (including social media, VOIP and messaging apps).

Chances are that you can easily spot the majority of spam communications and delete them without opening. However, cybercriminals continue to find new and innovative ways to trick users and make their messages appear real or legitimate. It only takes one communication and one click to fall prey to a malicious attack.

Like phishing communications, spam usually asks the recipient to provide sensitive and confidential information, so it can be used for malicious intents. Spam will often contain attachments that are malicious – for example a virus. Most spam filters include virus scanning, but new viruses appear by the hundreds every day and not all are recognised.



Social engineering

Social engineering attacks are an ever-present danger for organisations, because they target the one thing that is the hardest to control: employees.

These attacks manipulate the target into taking some form of action, which often include providing confidential or restricted information such as account credentials. Common examples of social engineering attacks include emails that look normal but contain malicious attachments or hidden links with viruses (phishing emails), pretending phone calls where the cybercriminal acts like a trusted source and then engages the employee to divulge sensitive information, and searching unlocked trash and recycling bins to discover valuable information that could be used in a future attack.

Nearly one million malware threats are released everyday...

Malware

CNN Money Report[4] revealed that there are nearly one million malware threats released each day. Malware is a general term for a program or file that is malicious and harmful to a computer and its user, including viruses, worms, Trojan horses, and spyware. Malware is known for infecting computers and corrupting information files, spying, as well as taking over the computer system.

Let's break down the types of malware attacks one by one.

- Viruses. This is the most common form of malware. A virus can be defined as a program that infects programs and files. Viruses, like Worms and Trojan horses can run programs as an administrator on devices, even Mobile devices. Some may be just malicious – interfering with the behaviour of the device. Others can collect information from the device and send that back to a control server, so the hacker can harvest personal or business information.
- Worms. These can spread through a system or server without any interaction, making them very dangerous.
- Trojan horses. These appear as authentic programs, but when they are installed they become malicious.
- Spyware. This malware collects user information and information and monitors their activity (even the built-on camera, speaker or microphone) without the user knowing. The collected information is then sent to a server operated by the spyware developer. It may include keylogging software.
- Ransomware
- Rootkits
- Crypto-jacking scripts

[4]http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html

SQL Injection Attack to communicate with databases

SQL stands for Structured Query Language; it's a programming language used to communicate with databases. Many of the servers that store critical information for websites and services use SQL to manage the information in their databases. An SQL injection attack specifically targets this kind of server, using malicious code to get the server to divulge information it normally wouldn't. This is especially problematic if the server stores private customer information from the website, such as credit card numbers, usernames and passwords (credentials), or other personally identifiable information, which are tempting and lucrative targets for an attacker.

An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if an SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords for the site. Like many infrastructure services, it is critical that the SQL server is running the latest software release to reduce the exploitation of SQL vulnerabilities.

Cross-Site Scripting (XSS)

In an SQL injection attack, an attacker goes after a vulnerable website to target its stored information, such as user credentials or sensitive financial information. But if the attacker would rather directly target a website's users, they may opt for a cross-site scripting attack. Like an SQL injection attack, this attack also involves injecting malicious code into a website, but in this case the website itself is not being attacked. Instead, the malicious code is taking advantage of an XSS vulnerability in the website design. The malicious code the attacker has injected only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website.

One of the most common ways an attacker can deploy a cross-site scripting attack is by injecting malicious code into a comment or a script that could automatically run. For example, they could embed a link to a malicious JavaScript in a comment on a blog.

Cross-site scripting attacks can significantly damage a website's reputation by placing the users' information at risk without any indication that anything malicious even occurred. Any sensitive information a user sends to the site—such as their credentials, credit card information, or other private information—can be hijacked via cross-site scripting without the website owners realising there was even a problem in the first place.

Session Hijacking and Man-in-the-Middle Attacks

When you are on the Internet, your computer has a lot of small back-and-forth transactions with servers around the world letting them know who you are and requesting specific websites or services. In return, if everything goes as it should, the web servers should respond to your request by giving you the information you're accessing. This process, or session, happens whether you are simply browsing or when you are logging into a website with your username and password.

The session between your computer and the remote web server is given a unique session ID, which should stay private between the two parties; however, an attacker can hijack the session by capturing the session ID and posing as the computer making a request, allowing them to log in as an unsuspecting user and gain access to unauthorized information on the web server. There are a number of methods an attacker can use to steal the session ID, such as a cross-site scripting attack used to hijack session IDs.

An attacker can also opt to hijack the session to insert themselves between the requesting computer and the remote server, pretending to be the other party in the session. This allows them to intercept information in both directions and is commonly called a man-in-the-middle attack.

Credential Reuse

Users today have so many logins and passwords to remember that it's tempting to reuse credentials here or there to make life a little easier. Even though security best practices universally recommend that you have unique passwords for all your applications and websites, many people still reuse their passwords—a fact that attackers rely on.

Once attackers have a collection of usernames and passwords from a breached website or service (easily acquired on any number of black market websites on the internet), they know that if they use these same credentials on other websites there's a chance they'll be able to log in. No matter how tempting it may be to reuse credentials for your email, bank account, and your favorite sports forum, it's possible that one day one of them will get hacked, giving an attacker easy access to your email and bank account. When it comes to credentials, variety is essential. Password managers are available and can be helpful when it comes to managing the various credentials you use. If available for the webservices you use, ensure that you use 2 Factor Authentication (2FA). This typically sends a code to a device you own (like a mobile phone) to confirm your login was valid.

This is just a selection of common attack types and techniques. It is not intended to be exhaustive, and attackers do evolve and develop new methods as needed; however, being aware of, and mitigating these types of attacks will significantly improve your security posture.

TDoS

Telephony Denial of Service (TDoS) is based in the same principles of the general DoS; establish an overwhelming number of sessions with the target premise, to take it down.

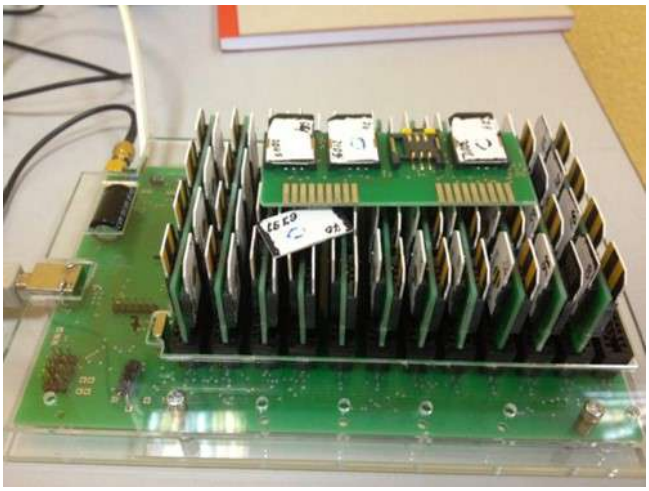
When the attack is forwarded to a private company, usually there is an economic reason and the attackers try to negotiate a ransom to stop the attack.

But when the attack is forwarded to a public service, such as police, 112, 911, etc. usually the target is not the money, so there is no attempt to negotiate.

This kind of attack is easier and cheaper to perform than DoS bound to a website, because of the easiness of obtaining distrained telephone numbers and putting them to use to make massive calls. The use of software -based PABXs in many enterprises has made it easier to perform these attacks.

There are simple, complex and distributed types of TDOS attacks depending on their nature. A simple attack uses some numbers in the same geographic area or same network to perform the attack, so usually it is easy to find and stop. Complex attacks can use more numbers and use a greater distribution. Distributed attacks can use a great number of lines, networks and form all over the country, so they can be very difficult to detect.

In October 2016, a powerful attack took place in the United States that impacted numerous PSAPs over 12 states. A simple manipulation in a seemingly innocent application caused smartphones to generate thousands of unwanted calls to 9-1-1 call centres and law enforcement agencies in multiple states.



Homemade device to generate TDoS attacks

In previous TDOS events toward emergency services, the attacks were directed more toward administrative telephone lines or "non-protected" 9-1-1 voice access lines, since calls to these numbers can be made from any telephone number.

There are no foolproof methods to detect and stop TDoS attacks, but some of the things that can be done to mitigate their effects include:

- Increase the capacity of the PSAP to hinder the attack.
- Keep an up-to-date analysis of your call history so it is easier to detect attack patterns.

Other solutions would involve telephony operators, as they could introduce filters that prevent a numberfrom placing repeated calls to 112, 9-1-1, etc.

In the case of an attack on a VoIP infrastructure, blocking or diverting calls based on a calling number is not an option. However, spoofing the IP address of the SIP source device is more difficult. Some prevention tools can detect a TDoS attack based on the source IP address and automatically block or divert TDoS calls while allowing legitimate calls to complete.

4. Who will attack you?

Before responding to a cybersecurity attack, you need to know what type of attacker you are dealing with. There are 6 main types, or "species", or cyberattackers:

THE THIEF

This is probably the most well-known type of cyberattacker, which usually involves someone stealing some type of login credentials or hacking a system or systems to steal sensitive information such as financial (i.e., credit card, bank account, etc.) or medical information.

THE RANSOMER

Typically referred to as "ransomware", this is digital extortion by the "ransomer". A type of malicious software ("malware") is used to block access to the victim's files or applications and makes them useless. The victim must pay a ransom to gain access or recover the files. This can be a targeted attack, or a random attack put out "into the wild" by individual hackers or organised crime. Petya is but one example in the alarming rise in the number of ransomware attacks.

THE DISRUPTER

These are attacks that are global in nature, wide-ranging and do not necessarily discriminate among governments, companies or individuals. The goal is to disrupt, sometimes just to show that "the disrupter" can do this. Taking down a website, disrupting Internet traffic or critical services, or even discovering and exploiting new vulnerabilities is practically sport for hackers and it earns serious bragging rights.

THE ACTIVIST

Whether it's protesting a belief, a cause, or an individual, these are the "hacktivists" that are making a statement. The attack can be political in nature or values-driven, ranging from organisations to individual hackers making their voice heard.

THE STATE

What used to be something you would see in the movies is now real-life. Whether it's government espionage or cyberweapons, politically motivated attacks range from spying to stealing intelligence, to sabotaging plots to actual cyberattacks.

THE ORGANISED CRIME ORGANISATION

The scariest of them all; from rogue hackers to terrorist organisations, this is where the connected world gets truly dangerous.

Cyberattacks may prevent citizens contacting emergency services...

5. Catalogue of impacts

Cyberattacks cause important impacts in organisations. Some examples are described in this section:

Interruption of service continuity/System disruption: If critical information and telecommunications systems are affected by a cyberattack, the service will be totally or partially interrupted. Additionally, access to the telecommunication system can be blocked and citizens will not be able to contact emergency services which may mean they do not receive timely medical or other assistance.

Information loss and confidential information reveal: Confidential and personal information are stored by emergency services.

Breach notification: In case of information loss, the organisation may be obliged to notify it to citizens and other stakeholders.

Note: Where General Data Protection Regulation (GDPR) applies there is a mandatory notification period

Brand, credibility and reputation damage: in case of service disruption, the image of the organisation will be damaged. Emergency services may lose their credibility and, as a consequence, the trust citizens have in them.

Forensic investigations, legal proceedings, fines and penalties: for example, a person not being able to reach emergency services may elect to start legal proceedings against the organisation and or its administrator(s).

Potential involvement in a cyberattack: Insecure Public Safety systems may be hijacked for attacks on other users and services, or for other activities such as crypto-mining.

The most important aspect: implementing long-term solutions

6. Measures to be taken

6.1 Before the incident

We have talked about different cyberattacks, what they are and their impacts, but the most important aspect to staying secure is to implement long-term cybersecurity solutions. These keep your organisation protected and can assist you if you ever are attacked.

For example, regardless of the method used to prevent DDoS attacks, the best time to implement a solution is before an attack happens, not during or after. Being aware and prepared is essential to mitigating DDoS and other

6.1.1 Risk Assessment Plan

Risk[5] is the likelihood that something bad will happen. For risk to exist, both a threat and a vulnerability that a 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 management must 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:

- Identify the Assets to be protected
- Identify existing and possible future threats (include human behavior)
- Assess existing and possible future vulnerabilities
- Assess risks: Risk assessment should extend beyond the Public Safety organisation to potential risks to the Internet and other Internet users (e.g. a compromised system could be used to attack others in the Public Safety network, or outside Internet users).
- Prioritise and Mitigate risks.

This continuum is depicted in Figure 1.

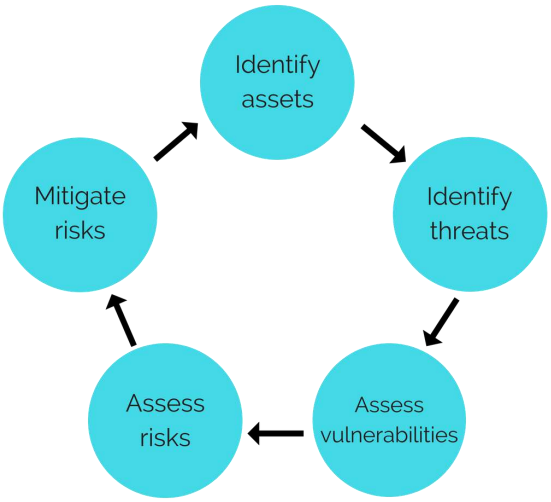


FIGURE 1: Risk Management Process[6]

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

[6]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.

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 other harm which would include infrastructure damage, customer information loss, and organisation reputation and likelihood of occurrence.

Organisations should include cybersecurity in the overall risk assessment plan, or, better, prepare a dedicated cyber risk assessment. An example or an approach to assessing cyber risk[7]:

Asset
What are you trying to protect?

Threat
What are you afraid of happening?

Vulnerability
How could the threat occur?

Mitigation
What is currently reducing the risk?

Impact / Severity
What is the impact to the business?

1. Negligible
2. Minor
3. Moderate
4. Major
5. Critical
6. Catastrophic

Probability / Likelihood
How likely is the threat?

1. Unforeseeable
2. Very Unlikely
3. Possible
4. Likely
5. Very Likely
6. Almost Certain

Risk Log

[7] http://www.ruleworks.co.uk/riskguide/security-risk-log.htm

Risk Log

Risk Log - Example of Security Hazards				Tolerability Level 12
Priority	**Hazard**	**Impact** (1-6)	**Probability** (1-6)	**Risk Rating** (Impact * Probability)
1	Information 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 cost and impact of damaged equipment, or equipment that needs to be taken out of service or replaced, needs to be taken also into account. For example, ransomware impact or webservers that need to be replaced after an attack. During the time of replacement an entire service could be unavailable.

The risk assessment plan should be used 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.

Controls can be physical, logical and administrative.

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.

Physical controls are those controls that protect the physical environment in which systems are installed or information 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 applications, systems, networks, and environments that process, transmit, and store information. 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 organisation promulgating them does not possess the authority to enforce them they are worse than useless.

What security policies should be established?

6.1.2 Policy

It is necessary to establish security policies and raise awareness of risks and best practices.

Have an **information security policy** (and communicate it). An information security policy should be used to define approved methods to securely transfer or share information and define restricted methods to help stop the use of unsupported or unsafe services and applications. They should include information about email policies, mobile devices, social networking, how to detect scams and malicious threats, and internet usage. These policies should be documented, communicated (multiple times), enforced, and periodically tested, audited, reviewed and updated. It should favour the use of encryption technologies and techniques to authenticate users and restrict access. Further, it should also require data minimisation practices

Understand **user agreements signed with your provider and conduct due diligence to ensure they are providing what they promise**. All information hosting services have user agreements that outline their terms and conditions. While these may be arduous to read, it is important to recognise and understand the fine print. You need to be careful you are not consenting to allow the provider direct access or ownership to your business information and customer information. In addition, it's important to understand third-party security policies and standards to protect your information within their hosting environment.

To include a **vendor check for a conflict of interest** where vendors sell data for advertising revenue would reduce the risk of data misuse and improve safety.

Finally, organisations need to have a **comprehensive incident response policy** that is the basis for actions taken detect and to identity an incident, contain the incident, preserve key forensic evidence, and communicate with partners and law enforcement. Much of this is described below in section 6.2, but it should be a formal policy with clear roles, obligations and stakeholders identified.

Include cybersecurity in tenders: Information and telecommunication system to be purchased or updated by the organisation, should follow the "security by design"[8] principles. This has to be clearly specified in tenders emergency services may publish.

[8]https://www.owasp.org/index.php/Security_by_Design_Principles

Once employees know how to stop attacks, the risk decreases...

6.1.3 People & education

Conduct security awareness trainings. Creating a culture around information security can help prevent a lot of breaches. One way to start is to make security awareness training a mandatory event for employees. This training should not only show employees the different kinds of cyber and social engineering attacks, but also show them how to thwart the attacks. Give concrete examples of actual threats, and possibly set up audits using a test/false attack to identify employee behaviors and then give additional training based on the outcomes. Once employees know how to stop these attacks before they even happen, the risk of a cyberattack decreases and will validate the criticality of your organisation's information.

Job description: a person in the organisation should be assigned as responsible for cybersecurity. Additionally, other people must be involved in cybersecurity. Different roles are needed, for example administrator of the spam firewall or post-incident processes specialists.

Limit administrative access: Do not allow employees to have administrative account access, unless mandatory or required based on staffing duties and responsibilities.

Communication Plan: Having a communication plan is necessary, since it will be necessary to contact specific individuals or providers during an incident.

Tools: make sure the team that will deal with the incidents will have the right roles and tools.

6.1.4 Technical Measures

Evaluate the computing infrastructure by performing such tasks as proactive scanning and network monitoring, and by performing security and risk evaluations. Run port scanning tools across your network devices to ensure only the ports that are required to run the operation are open to the Internet. Many hackers gain access to key internal resources through open ports on internal servers. Restrict and closely monitor ports used by third party external contractors.

Hire an independent security audit specialist to periodically (e.g. at a minimum once a year) review IS-IT infrastructure and, security policies to identify weaknesses in these key elements of cybersecurity protection and detection.

A VPN can allow a secure connection wherever you are...

Implement infrastructure **protection improvements resulting from these audits or reviews** or other process improvement mechanisms.

When connecting from outside the PSAP, using a trusted **Virtual Private Network (VPN)** allows you to have a secure connection wherever you are, whether at home, a coffee shop, or in the airport. A VPN encrypts your connection, making anyone else on the same Wi-Fi network unable to intercept your traffic. A quality, business-grade firewall will have VPN capabilities. In addition, there are many hosted services that offer VPNs.

Services such as **anti-virus, firewall protection, network monitoring, and wireless security** are layers of defense to give you state-of-the-art protection. Having a network that is protected behind a firewall and an elaborate network architecture is a necessity and can be the difference between being hacked and being safe. Most organisations have a firewall, but not all of them are using their firewall to its full potential. A firewall is the foundation to protecting your network from unauthorized access. A business-class firewall can perform additional services like blocking dangerous or unproductive websites, running in-depth reports showing which websites your employees are visiting, bandwidth consumption, and other information that can impact productivity.

With a special focus on current developments in the telephony domain, the move from ISDN access lines to SIP trunks (Session Initiation Protocol), thus calls moving from dedicated voice networks to Voice over Internet Protocol (VoIP) and the PABX becoming more and more a software function on generic IT infrastructures, real-time communication with voice and video traffic needs become an integral part of the security assessment and risk mitigation activities. Where applications involving non-real-time traffic to the PSAP can be protected by the above-mentioned mechanisms like VPN and firewall, any kind of SIP-based traffic must pass through **Session Border Controllers** (SBC).[9] Session Border Controllers define a dedicated service demarcation point for the SIP traffic between the PSAP and the public network – in analogy to the firewall protecting the corporate application platforms against attacks from the Internet. Key features of an SBCs are SIP session inspection capability that traditional firewalls don't have, detection of typical attack patterns and protecting against SIP-based TDoS attacks, as well as voice and video session encryption in analogy to VPNs securing the data traffic.

Going one step further is the use of **Unified Threat Management**. This is a more comprehensive approach, where multiple security functions work within a single platform. A firewall is part of Unified Threat Management, but this capability also includes: network intrusion detection/prevention, anti-virus, gateway anti-spam, VPN, content filtering, load balancing, information loss prevention, and reporting.

Invest in **intrusion detection systems (IDS) and /or log management tools**, most important of which is a class of products call Security Infrastructure and Event Managers (SIEM). These tools are critical for both identification of incidents and for forensic analysis after the fact.

Invest in a log management tool to monitor server and network activity. This tool can provide alerts about possible cybersecurity incidents.

Many organisations see the benefit to a **managed security service** because it provides more time for internal resources to focus on core business functions and initiatives and allows them to run everything through a single vendor. With a managed service provider constantly monitoring and updating your network, your organisation will improve efficiency and productivity.

[9]EENA Long Term Definition Document: http://www.eena.org/ressource/static/files/2013-03-15-eena_ltd_v1-1_final.pdf

To ensure maximum protection, it's best practice to encrypt your information while in transit and at rest. **Encryption** renders information unreadable when accessed without possession of an encryption key, access to which can be controlled and provided to only authorized users. Having a process in place that ensures sensitive devices use encryption, keys are stored securely, and that files and emails are being properly sent is imperative. Ensure that all web servers used by the organisation force Secure Sockets Layer (SSL) for Web connections, ensure email servers enforce Transport Layer Security (TLS), and have end users add extensions to browsers such as SSL-Everywhere to force SSL connections to external websites.

Encryption renders information unreadable when accessed without authorisation...

Implement changes to the computing infrastructure to stop or mitigate the potential exploitation of a vulnerability in the hardware or software infrastructure, if needed. For example, the network of core applications of the PSAP should be isolated from the network used for emailing and web browsing.

Update your software as soon as any update is available. Many commercial software solutions – operating systems, browsers, firewalls, spam filters - automatically update the software with every new release. Don't disable the automatic update feature of these solutions. Do not wait to install available updates to your software, browsers, and plugins. Updating regularly when updates become available increases your safety, because many times this will help patch any security vulnerabilities.

Have the right hardware. To prevent DDoS attacks, you also need the appropriate hardware to mitigate these kinds of cyberattacks. Managed firewall solutions can defend your organisation against many kinds of DDoS attacks, allowing you to have peace of mind that your network and servers are safe.

Use **strong passwords**. To prevent malware from infecting your computers, create a strong unique password that can't easily be cracked, and make sure you always log out of websites. Where possible use 2 Factor Authentication (2FA).

Are you regularly backing up information?

Spread out your servers. Having your servers in different data centres that are on different networks ensure that your information and servers are dispersed throughout several locations. That way, the impact of a targeted attack does not affect all your servers. It is also helpful for resiliency in the event of a natural disaster.

Ensure **your organisation is not the source of DDoS attacks**. This is an additional reason for taking preventive steps, such as installing and maintaining anti-virus software, performing timely system updates, and ensuring firewalls and network devices are properly configured.

Perform cybersecurity tests[10]: penetration tests will find vulnerabilities in the system that an attacker could exploit.

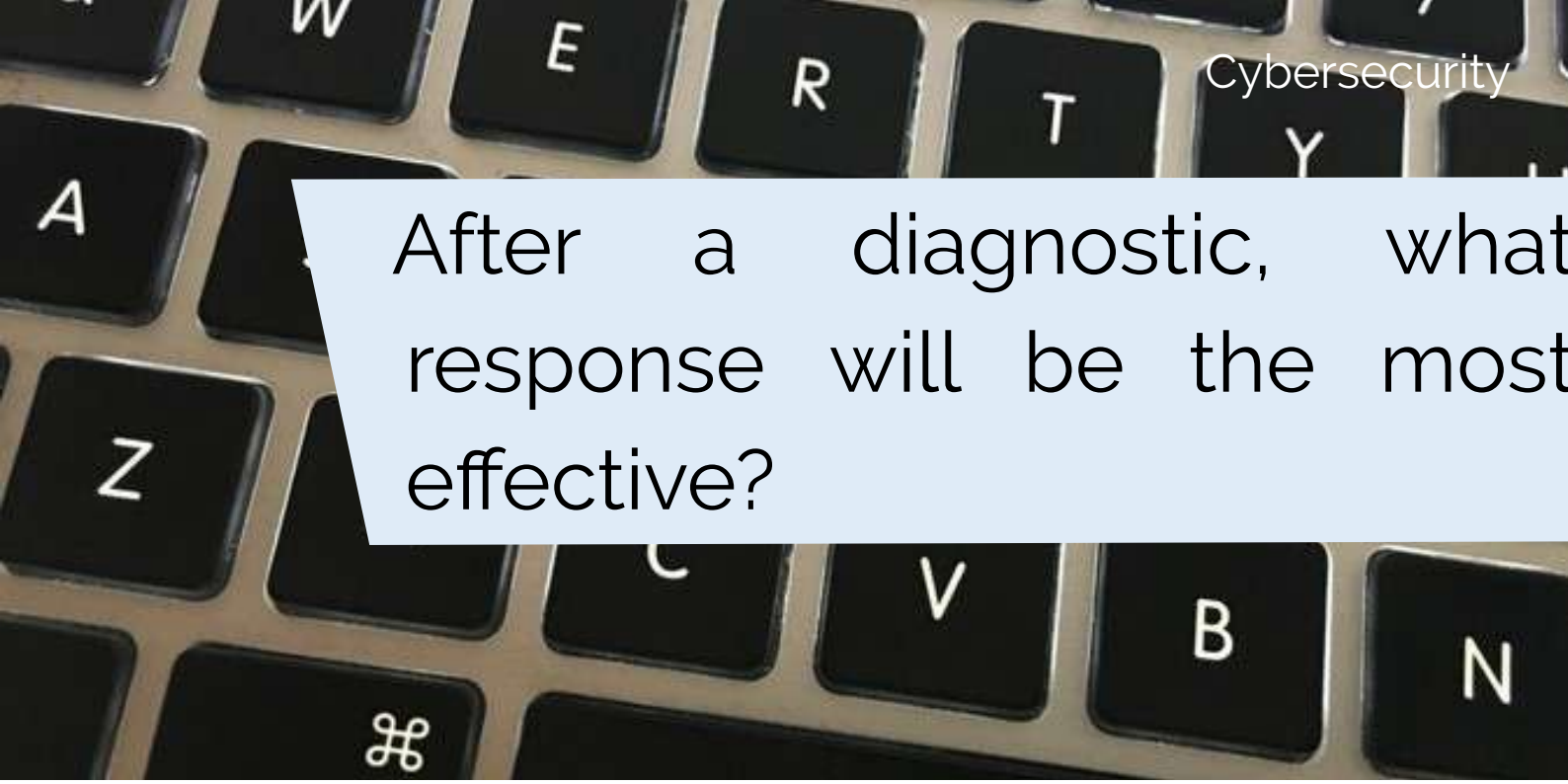
Back up regularly: Make sure you're backing up information on a regular basis, to ensure that the backups are operating as planned and can be efficiently restored. Do more than one back-up, and ensure one is stored off-site (i.e. in another location).

Have software restrictions: Prevent ransomware attacks from infiltrating and running common programs with a software restriction policy or put access controls in place. Do not give individual users with administrator access privileges to their computers.

Eliminate macros: Macros automatically perform frequent tasks, but they can be disabled. Disabling macros will ensure malicious content doesn't automatically load.

Block internet ads: Many third-party ads have some type of malware. It's best to avoid the risk by disabling all internet ads on devices.

[10]https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf



6.2 During the incident

6.2.1 Introduction

Once the organisation is being attacked, the first logical step is to detect it. After this, a diagnostic of what is happening is needed to know what response can be most effective.

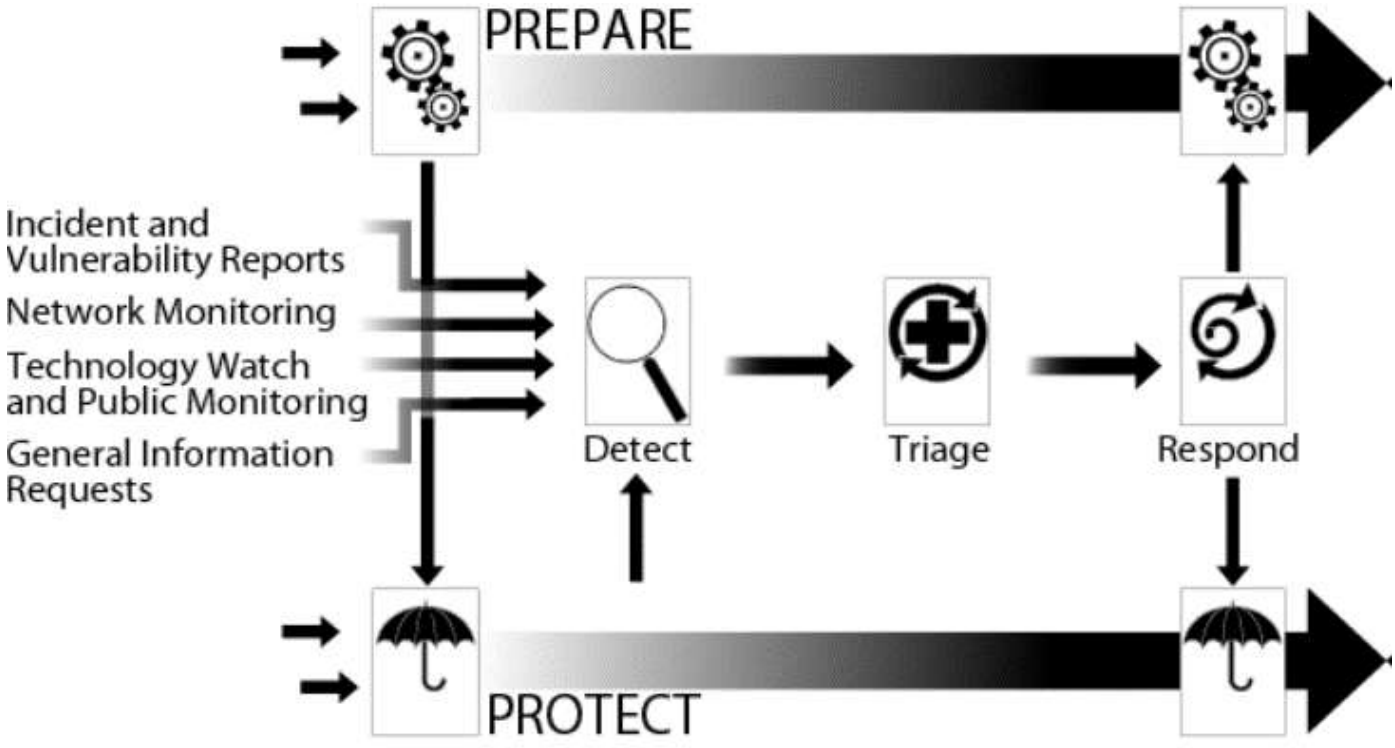


Figure 2

6.2.2 Detect / Identify

Many cybersecurity incidents are about stealing critical / confidential information – often by state-sponsored actors or organised by cybercrime gangs – that are looking to obtain intellectual property or other sensitive information. As a result, they are mostly non-destructive (although some are very destructive), unobtrusive and difficult to detect (often because attackers have covered their tracks).

Cybersecurity incidents may also take place over a long time or in different locations of where the organization operates. Advanced targeted attacks can go undetected for many months or years, and even when discovered are often assumed to be nothing more than a common malware infection. Equally, many variants of credential stealing Trojans can remain undetected for many months at a time.

There are many ways in which a cybersecurity incident can be identified (with varying levels of detail and accuracy), which include:

- Alerts generated by technical monitoring systems, such as Data Loss Prevention (DLP), intrusion detection systems (IDS), antivirus software, and log analysers or security information and event management (SIEM) tools.
- Suspicious events reported, for example, to the IT help desk by users; to account managers by third parties (often customers); or directly to the security team by industry bodies, your vendor partners or the government.

Other good practices are:

- Notice events or anomalies detected by audits, investigations or reviews.
- Receive the reports of events
- Proactively monitor indicators such as network monitoring, IDS, or technology watch functions
- Analyze the indicators being monitored (to determine any notable activity that might suggest malicious behavior or identify risk and threats to the enterprise infrastructure)
- Forward any suspicious or notable event information to the Triage process
- Reassign events to areas outside of the incident management process if applicable
- Close any events that are not forwarded to the triage process

6.2.3 Triage

The early part of an investigation is often referred to as Triage, which consists of:

- Indentifying a suspected cybersecurity incident (e.g. monitoring evidence of unusual occurrences and assessing one or more trigger points)
- Classifying cybersecurity incidents (e.g. critical, significant, normal or negligible impact)
- Prioritising these incidents (e.g. high, medium or low)
- Assigning incidents to appropriate personnel in terms of their legitimacy, correctness, constituency origin, severity or impact.

-categorize and correlate events

-prioritize events

-assign events for handling or response

-pass on relevant information and information to the Respond process

-reassign events to areas outside of the incident management process if applicable

-close

Category	Description	Example
Critical	These incidents will usually cause the degradation of vital service(s) for many users, involve a serious breach of network security, affect mission-critical equipment or services or damage public confidence in the organisation.	Targeted cybersecurity attacks or loss of publicly available online service.
Significant	Less serious events are likely to impact a smaller group of users, disrupt non-essential services and breaches of network security policy.	Website defacement or damaging unauthorised changes to a system.
Minor	Many minor types of incident can be capably handled by internal IT support and security. All events should be reported back to the information security team who will track occurrences of similar events. This will improve understanding of the IT security challenges and may raise awareness of new attacks.	Unsuccessful denial-of-service attack or the majority of network monitoring alerts.
Negligible	It is not necessary to report on incidents with little or no impact or those affecting only a few users, such as isolated spam or anti- virus alerts; minor computer hardware failure; and loss of network connectivity to a peripheral device, such as a printer.	Isolated anti-virus alert or spam email.

6.2.4 Respond

The top challenges faced by organisations when trying to identify a cybersecurity incident and respond to it in a fast, effective and consistent manner include some tasks that can be done before an incident strikes and some that must be taken after an incident is identified. Steps that should be taken to prepare an organization to respond to an identified incident BEFORE it occurs include:

- Assigning an executive to have ongoing responsibility for the Incident Response (IR) plan and for integrating IR efforts across business units and geographies.
- Developing a taxonomy of risks, expected threats, and potential failure modes and refresh them continually based on changes in the environment.

What are the challenges faced by organisations?

- Developing quick-response guides for likely scenarios and make them easily accessible.
- Establishing processes for making major decisions, for instance, when to isolate compromised areas of the network and how to do so quickly.
- Maintaining relationships with key external stakeholders, such as law enforcement (for example, in the United States, the Federal Bureau of Investigation).
- Maintaining service-level agreements and relationships with external breach-remediation providers and experts.
- Ensuring that documentation of IR plans is available to the entire organisation and is routinely refreshed.
- Ensuring that all personnel understand their roles and responsibilities in the event of a cyberattack.
- Identifying the individuals who are critical to incident response and ensure that they have backup and that a succession plan is in place.

Steps to take to respond to, or mitigate, an incident once it is determined that an incident is, or has, taken place include:

- Analysing all available information related to the potential cybersecurity incident
- Determining the complete set of compromised machines and servers using SIEM information where possible.
- Determining what has happened (e.g. a DDOS, malware attack, system hack, session hijack or information corruption)

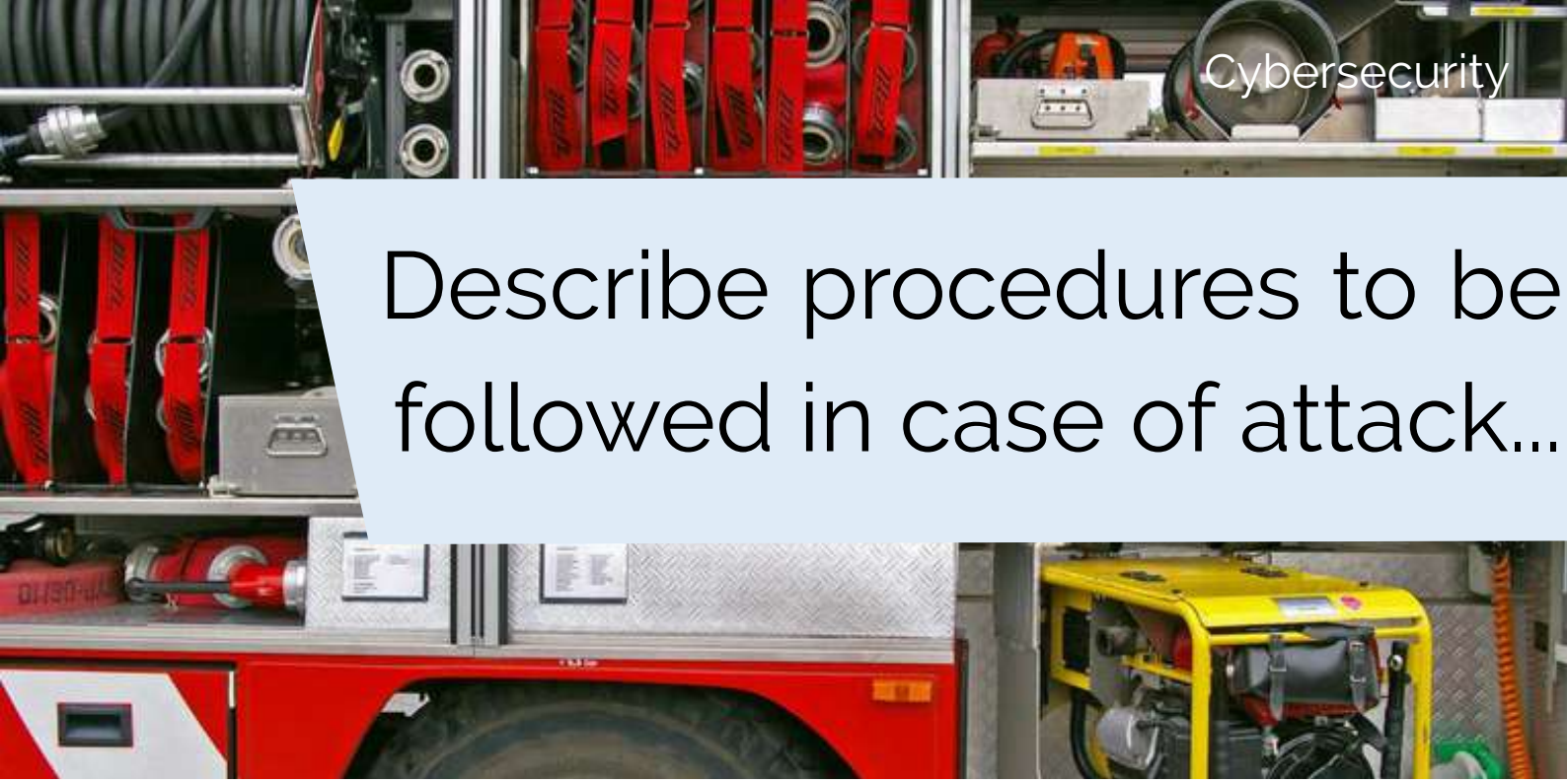
Develop quick-response guides for likely scenarios...

- Coordinating and providing technical, management, and legal response, which can involve actions to contain, resolve, or mitigate incidents and actions to repair and recover affected systems
- Communicating with external parties (like service providers, vendors, etc.)
- Isolating compromised devices immediately by removing them from the network as soon as possible to prevent ransomware from spreading to the network or shared drives.
- If the network has been infected, immediately disconnecting all connected devices.
- Isolating the infected devices from the network, but should be leaving them running. Important forensic information may be deleted if the machine is turned off and later back on. If the source of the intrusion or compromise is to be determined, the suspect device needs to be left running.
- Backed up information should be stored offline. When an infection is detected, take backup systems offline as well and scan backups to ensure they are free of malware.
- Contacting law enforcement immediately to report any ransomware events and request assistance.

6.3 After the incident

Once the attack is under control, it is time to analyze the causes and weaknesses that led to the attack. It also necessary to quantify damages and other actions like:

- Mobilise crisis management team with support from communications and legal advisers, as appropriate
- Record the date and time when the breach was discovered, as well as the current date and time when response efforts begin, e.g. when someone on the response team is alerted to the breach
- Secure the IT systems affected by the cyber-attack to help preserve evidence
- Stop additional information loss. Take affected equipment offline (in isolation) but do not turn them off or start probing into the computer until your forensics team arrives
- Document everything known thus far about the attack
- Interview those involved in discovering the breach and anyone else who may know about it. Document your investigation
- Review protocols regarding disseminating information about the breach for everyone involved in this early stage.
- Assess priorities and risks based on what you know about the breach
- Bring in your forensics team to begin an in-depth investigation
- Protect your reputation with an internal and external communications strategy, supported as necessary by crisis communications specialists and/or reputation lawyers
- Report to police, if/when considered appropriate
- Notify regulators, if needed, after consulting with legal counsel and upper management.
- Notify insurance broker(s) to ensure compliance with policy terms.



Describe procedures to be followed in case of attack...

7. EENA recommendations for public authorities

Item	Actions	Stakeholder
Risk assessment plan	Include cybersecurity in the general risk assessment plan Use templates, the latest standards and checklists derived from industry best practices wherever possible Involve all stakeholders	Public Authorities
People	Have a person responsible for cybersecurity assigned within your organisation Initiate and maintain a robust internal security training program Include human behaviours in the risk assessment plan	Public Authorities
Testing	Perform penetration testing that also includes social media	Public Authorities
Technology	Consider the inevitable need for connecting your systems to the public Internet in the future Use standard security stress-tested architectures wherever possible	Public Authorities Vendors
Tenders	Consider security in tenders – "bake-in" security by design Ensure your vendor adheres to their own strict standards including their behaviour standards	Public Authorities
Contingency plans	Make sure there is a plan in case of attack (include Telephony DoS) Describe protocols and procedures to be followed in case of attack	Public Authorities

8. References

- Incident Handler's Handbook
- ISO/IEC 27035:2011
- Nist SP800-86
- Incident response process best practice. (2008, September 25). Retrieved from http://security.tennessee.edu/pdfs/IRPBP.pdf
- Responding to it security incidents. (2011). Retrieved from http://technet.microsoft.com/enus/library/cc700825.aspx
- Creating a computer security incident response team: a process for getting started. (2006, February 27). Retrieved from http://www.cert.org/csirts/Creating-A-CSIRT.html
- Bejtlich, R. (2005). The tao of network security monitoring: beyond intrusion detection. Boston, MA: Pearson Education, Inc.
- Incident handling step-by-step and computer crime investigation. (2011). Retrieved from http://www.sans.org/security-training/incident-handling-step-by-step-computer-rimeinvestigation-day-1-799-cid
- Uf it security incident response procedures, standards, and guidelines. (2011, July 13). Retrieved from http://www.it.ufl.edu/policies/security/uf-it-sec-incident-response.html
- Newman, R. (2007). Computer forensics: evidence collection and management. Boca Raton, FL:Taylor & Francis Group, LLC.
- Handbook for CSIRTs, CMU/SEI-2003-HB-002 [West-Brown 03]
- Organisational Models for CSIRTs, CMU/SEI-2003-HB-001 [Killcrece 03a]
- State of the Practice of CSIRTs, CMU/SEI-2003-TR-001 [Killcrece 03b]
- https://www.neustar.biz/blog/marketers-5-things-Cyberattack