Co-funded by the
Erasmus+ Programme
of the European Union

Template for InCyT Training Modules

Information Security for Managers Unit 3 -Week 6 Unit (Module) name: Third party vendor security	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• George Matache – et al.
Learning Activity Goals	1. Risks in Social Networks 2. Measures to have Security and Privacy in Social Networks 3. Security techniques 4. Procurement requirements
Skills to be Gained	• TS3 Network Security • TS4 Penetration (exploitable vulnerabilities) testing • SS3 Cognitive and behavior analysis
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Basic management skills • Basic IT skills • Basic security skills

Brief information about the module

Description
Procurement requirements refer to the goods and services that must be acquired from organizations outside the performing organization. For a variety of reasons, sometimes performing organizations rely on vendors to provide what's needed to complete a project. For example, consider the widget manufacturer that undertakes a project to automate their inventory tracking system. Some of the project work activities involve the relocation of storage bins in their main warehouse. Some of the work activities involve custom software development. As to the software development activities, widget manufacturer doesn't have a human resource who knows how to develop the software application. Regarding the software development activities, widget manufacturer must procure those services. Web-based social networks (WBSNs) are online communities that allow users to publish resources (e.g., personal data, annotations, blogs) and to establish relationships, possibly of a different type for purposes that may concern business, entertainment, religion, dating, and so forth. In the last few years, the usage and diffusion of WBSNs has been increasing, with about 300 Web sites collecting the information of more than 400 million registered users. As a result, the "net model" is today used more and more to communicate, share information, make decisions, and 'do business' by companies and organizations. It is then a challenging issue to devise security mechanisms for social networks, able to protect private information and regulate access to shared resources. In this article, besides providing an overview of the characteristics of the WBSN environment and its protection requirements, we illustrate the current approaches and future trends to social network security, with particular attention paid to the emerging technologies related to the so-called Web 2.0. The learners could be informed about such aspects by reading the corresponding text, watching streaming webinars and solving exercises at own pace. All these documents are on the digital interactive project platform. The learners can test their answers on Self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forum and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the meetings. They will be supported to develop e-portfolio important for reflection and evaluation of the training.

Content of the Learning Material (🕓 ?? minutes or 10-12 pages)

A third-party vendor is a person or company that provides services for another company (or that company's customers). While vendors are considered "third parties," some industries differentiate a "third-party vendor" specifically as a vendor under written contract, but not all vendors work under a contract. For clarity's sake, the term "third-party vendor" in this article refers to any individual or company that provides services to another company with or without a contract.

Cooperation is the key to success. Working with third parties helps businesses increase their productivity and efficiency, produce better products and services, employ highly qualified experts, and cut costs. But all these benefits come at the price of increased cybersecurity risks. Minor flaws in your third-party vendor's security and privacy routines may turn into cybersecurity weaknesses for your company. In this article, we analyse the particular cybersecurity risks related to third parties and how you can mitigate them.

Goods and services obtained from third-party vendors can include, but aren't limited to:

- Cloud web hosting services. A cloud hosting vendor might provide everything from disk space and bandwidth to encryption and high-tech security solutions.
- Cloud-based software solutions. SaaS software vendors provide access to software programs either for your business or your customers. For example, marketing automation platforms, CRMs, accounting packages, etc.
- Equipment maintenance. The company that fixes your copy machine and the team that manages your network security are third-party vendors.
- HVAC servicing. The local HVAC company that services your unit is providing third-party vendor services.
- Contractors of any kind. Any contractor, short- or long-term, is a third-party vendor.
- Call center providers. If you host your call center with another company, it is considered a third-party vendor.
- Bookkeeping/financial auditors. Any person or business hired to manage your finances, budget or audit your finances is a third-party vendor.
- Lawyers. Sometimes it's necessary to consult a lawyer before signing contracts or making big purchases. All legal services are considered third-party vendors.

As organizations increasingly rely on third-party vendors to provide essential services, they also become more vulnerable to vendor related cybersecurity risks. A recent study found that nearly 60% of companies experienced a data breach due to a third-party vendor in the past year. But what are the most common vendor cyber gaps that organizations should be aware of?

What are the benefits of using third-party vendors for service providers?

In today's world, it's impossible to avoid using third-party vendors. No matter how many departments your company creates, you'll never cover every service you'll ever need. Nor should you, as companies must determine the right balance of skills that are essential to the business versus those that can be outsourced. Here's what happens when you get that balance right:

You will save time. Nobody has time to learn every skill or hire every person necessary to run a business. Third-party vendors make business processes run smoothly by obtaining all the professional services required to operate and fulfil orders for your customers.

You will save money. Perhaps the biggest benefit is the cost savings. Contracting a third-party provider for work as needed can be significantly less expensive than always having professionals on company payroll. For instance, it's far less expensive to hire a lawyer when you need one rather than keep a lawyer on retainer.

You will get valuable expertise. Your company doesn't have time to develop a new team of experts. The time and cost of doing so would be enormous. Hiring a third-party vendor for expertise you don't have in-house will likely yield better results.

What are the risks of using third-party vendors?

Third parties may not take their network security as seriously as you want them to. Knowing this, hackers may choose not to attack your company directly. Instead, they may look for an easier target among your third-party vendors. A compromised subcontractor can easily be turned into an entry point for cybercriminals.

If your vendors fail to deliver, you will fail to deliver. However, risk is inherent in any business relationship. Using third-party vendors comes with many risks, most of which can be mitigated.

The biggest risk is choosing a third-party relationship that does not align with your security standards. For instance, your network security team needs to follow security protocols that live up to your specific standards. If your company is bound by regulations such as health insurance, you cannot afford to hire a network security company that does not comply with the health insurance regulations. You need a vendor that understands regulations and is willing to adapt to meet those regulations.

When you are bound by data privacy regulations, you need to know exactly what security standards are being implemented and if your vendors are not on par with them, you must try to remediate that. Otherwise, you are exposing your company to cybersecurity risks such as a data breach.

Data breaches are extremely disruptive, especially when you're protecting personal information. Unfortunately, data breaches are on the rise and are more common than ever before. Data breaches can cause disruptions to operations, devastating financial consequences, legal action and a damaged reputation. To avoid these, you cannot let your guard down when it comes to your own security or that of your vendors.

Depending on the nature of third-party vendor compromise, an organization may face different risks. Let us look at the most common risk categories and the threats you need to be prepared to mitigate. A compromised third-party vendor may lead to multiple risks that can be split into four major categories: Fig 1

Cybersecurity risks — Subcontractors usually have legitimate access to different environments, systems, and data of their clients. Attackers may use a third-party vendor as an entry point to try to get a hold of your valuable assets.

Operational risks — Cybercriminals may target your internal systems and the services you use instead of just your data. This can lead to partial interruptions of your operations or even halt them altogether.

Compliance risks — International, local, and industry-specific standards and regulations set strict cybersecurity criteria that organizations should meet. Furthermore, third parties working with these organizations also have to comply with these requirements. Non-compliance usually leads to substantial fines and reputational damage.

Reputational risks — Having your valuable data and systems compromised serves as a red flag for

your partners and customers, both current and future. Regaining their trust will take a lot of time and effort. And unfortunately, there's no guarantee that you'll be able to successfully recover your reputation after a severe cybersecurity incident.

Procurement requirements

For a variety of reasons, sometimes performing organizations rely on vendors to provide what's needed to complete a project. Especially, the SMEs. Procurement requirements are therefore of utmost importance to work with third party vendor security.

While it's true that procurement is a highly individualized process, there are also several foundational stages that will generally be utilized across the board.

Procurement requirements refer to the goods and services that must be acquired from organizations outside the performing organization. For a variety of reasons, sometimes performing organizations rely on vendors to provide what's needed to complete a project.

The Stages of Procurement
Stage 1: Identify a need for products and/or services.
Stage 2: Create and submit a purchase request.
Stage 3: Evaluate and select suppliers/vendors.
Stage 4: Negotiate the terms of a contract with the selected supplier.
Stage 5: Finalize a purchase order.

The first step in the procurement process is to identify requirements. All procurement requirements begin with the perception of a need. The need to cross a body of water could create a requirement to build a bridge, a ferry, or other transportation systems.

Stage 1: Identify a need for products and/or services
Before the procurement process can begin, a specific need must be recognized. For example, an organization may be interested in purchasing new computer monitors, re-ordering their monthly supply of paper products, or acquiring updated software. Depending on the company structure, this step might be managed by the business owners, department heads, executive team, staff, and/or procurement managers. In this stage, a budget will be set and a comprehensive view of spending will often be assessed.

At this stage it is necessary to clearly define the need, and this may be done by way of a study to determine the best mode to cross the body of water (given the present situation and forecasted future need), then the type of bridge to be constructed, or a comparative cost/benefit analysis to determine the best solution between a bridge and other alternatives. The study should include if

the need can be satisfied in-house or contracted out, quantification of the initial budgetary estimate, and an idea of the procurement lead-time.

Stage 2: Create and submit a purchase request

A purchase request (or purchase requisition) is a formal request for goods or services and is generally submitted using specialized procurement software. Oftentimes, the purchase request will originate with an employee or manager, then be reviewed by the organization's procurement team.

When a purchase request is approved, it becomes a purchase order. However, should the request be denied, it will typically be returned to the submitter with a brief explanation. A rejected purchase order, while not ideal, can be a good learning opportunity.

Stage 3: Evaluate and select suppliers/vendors

The next step is to assess various vendors, then choose one that meets key requirements. Some organizations maintain a catalogue of approved vendors, featuring various suppliers that have already proven themselves.

Soliciting vendors is a process that can range from simple to complex, with its scope determined by the requirement(s) at hand. Usually, several requests for quotation (RFQ) will be sent to various vendors, so that the organization/procurement team can compare prices and options.

Remember that price should not be the only determinant when choosing a vendor. For best results, consider the "big picture" of what a vendor can offer, including:

- Ease of communication
- Company ethics
- Accountability
- Production capabilities

After a vendor has been selected, investing time and energy into the relationship is important. A good relationship with a supplier can unlock better savings and service, delivering maximum value in the long term.

Stage 4: Negotiate the terms of a contract with the selected supplier

Once you have chosen the best-fit vendor, it's time to move on to contract negotiations. In terms of successful procurement, this is one of the most critical stages by far. It is in this stage that you will outline – and agree to – pricing, as well as details such as delivery schedules, specific terms and conditions, and more. It can often be useful to assess previous contracts to pinpoint opportunities for improvement, allowing you to take a more informed approach going forward.

Stage 5: Finalize a purchase order

After the final contract has been approved, the next order of business is the purchase order (PO). The contract typically governs the full buyer/supplier relationship, while a purchase order zooms in on a specific purchase.

- Think of this document as another formal contract, which fully details the following:
- Total costs/price
- Detailed description of the goods and/or services
- Quantity
- Any other specific terms and conditions

Stage 6: Order management

As the goods/services are delivered, there should be someone responsible, ideally the end-user of the product or services, for checking that all standards have been met delivery deadlines, product quantities, and quality, etc. If there are issues with the items (e.g. damaged products), you have the option to reject the delivery. Clear communication with the vendor is key in the event of any delivery problems.

As technology and communications allow businesses to expand their supply chains, the complexity of vendor risk management increases. Your business is likely working with more vendors than ever before, and each of those vendors is going to pose some level of risk to your organization.

Vendor security risk management is a strategy designed to limit the number of threats, vulnerabilities, and weaknesses your organization faces due to the vendors in your supply chain. A vendor is typically a third-party organization that sells a product, service, or piece of equipment that your business needs to operate.

Each vendor, upon being connected to your organization, is going to carry some level of cybersecurity risk. If they fail to uphold their end of the deal, or if they're the victim of a cyberattack, it could impact your organization directly. An effective risk assessment, as part of a greater vendor risk management plan, strives to identify these potential failure points long before they become a problem and fix them.

The Cycle of Vendor Risk Management

Vendor security risk management is an ongoing process, and one you'll execute with every vendor you bring into your supply chain. Typically, the process looks like this:

Step 1: Analysis – The company identifies the inherent risk of the relationship and the level of due diligence to be performed. Accordingly, the company evaluates the third party's security posture

and performs a gap analysis.
Step 2: Engagement – The company and third party collaborate on how to remediate gaps.
Step 3: Remediation – The third party fixes the cyber gaps.
Step 4: Approval – The company approves the third party or rejects it based on risk tolerance.
Step 5: Monitoring – The company continues to monitor the third party to detect any cyber gaps

Social networks and vendor security risks

Social networks are very popular in today's world. Usually, a social network is defined as a small-world network, consisting of a set of individuals (persons, groups, organizations) connected by personal, work, or trust relationships. Social networking is then a quite broad and generic notion, which in the Web context might be applied to any kind of virtual community. For instance, users registered to a Web service, such as Web mail, online journals, or newspapers requiring a subscription, can be considered as a social network. In the following, we adopt the definition, according to which an online community's Web site can be considered a Web-based social network only if it satisfies the following conditions:

- Relationships are explicitly specified by its members, and not inferred from existing interactions (e.g., a mailing list can be used to infer implicit relationships).
- Relationships are stored and managed by using technologies, such as database management systems, allowing relationship analysis and regulating access and retrieval of relationship data.
- Members are able to access relationship information, at least partially.

Key Terms

Relationship-Based Access Control: An access control paradigm specifically tailored to social networks, according to which social network members authorized to access a given resource are denoted in terms of the relationships they must participate in to get the access.

Social Network: A small-world network consisting of a set of individuals (persons, groups, organization) connected by personal, work, or trust relationships. Usually modelled as a graph, where nodes correspond to social network members, whereas edges denote the relationships existing between them.

Social networks. Communicating and sharing information with those around us is a part of everyone's life and has evolved from simple text messages to emails and to what we now call social media platforms. What is not very well known or realized is the fact that our exposure in the online environment comes with a lot of risks.

Social media and social networking or messaging applications can pose a number of security and privacy risks to both organizations and individuals when used in an inappropriate or unsafe

manner. The most popular and widespread platforms on social networks:

- Facebook with over 1,300,000,000 members;
- Flickr used to store, organize and share media files;
- LinkedIn with over 300 million users;
- Instagram with over 30 million users;
- Twitter with over a billion members;
- YouTube with over a billion users;
- Tinder with about 12 million users;
- TikTok with over 800 million users.

Privacy-Aware Access Control: In the context of social networks, denotes an access control paradigm where access control requirements of social network members are enforced without disclosing private information about the relationships they participate in.

Web-Based Social Network: A Web-based system that allows its registered members to establish relationships with other members and to share different types of information (e.g., personal data, contacts, multimedia resources).

Social Network Analysis: A discipline aimed at collecting statistical data from the analysis of social network topology.

Relationship Trust Level: In a social network, denotes the value associated with a trust relationship, providing a measure of how much a given member considers another member trustworthy. Depending on the purpose for which it is used, this notion may have different meanings. For instance, in a collaborative rating environment, it denotes how much a given member trusts the opinions of another member with respect to a specific topic (topical trust) or in general (absolute trust). By contrast, in an access control context, it has some similarities to the notion of security level used in mandatory access control models.

Edge Perturbation: Graph anonymization technique aimed at hiding the actual social network relationships by performing a set of random edge deletions/insertions in the network graph.

Social Network Relationship: A relationship concerning two members of a social network. In WBSNs, besides personal/work relationships (e.g., friend/colleague), also trust relationships may be supported which denote how much a one member trusts another. In the graph representation of a social network, relationships are usually denoted by edges, labelled with a relationship type and/or a relationship trust level.

Graph Anonymization: Technique aimed at hiding private information about social network

members when performing social network analysis. Node anonymization and edge perturbation are the two main graph anonymization techniques currently used.

Node Anonymization: Graph anonymization technique aimed at hiding social network members' identities by labelling the corresponding nodes with random identifiers (naïve anonymization), or, in case nodes are associated with attributes which can be used to identify the corresponding user, by using techniques based on k-anonymity (Sweeney, 2002).

Risks

Geotagging

- Represents the addition of geo-identifying data to photos, videos, websites and text messages by applications that can read your location or are allowed to do so in your settings;
- Be sure to turn off geotagging features in sensitive locations to avoid revealing your exact location, where you work, or where you live.

"Audience"

- It's a general term that refers to who is able to see and/or comment on your posts;
- Your friend group can change at any time and be able to view a post that contains information about you. You may intentionally share something with your "friends", but what they do with the post is beyond your personal control.

Identity

- Describes the range of information that specifically relates to an individual;
- It should be kept in mind that there are people who use social media as a research method to search for identity information, with possible malicious intent, such as identity theft, fraud, embezzlement or intimidation.

Measures

Password

- It is recommended to use a different password for each online account;
- It should be at least 10 characters long and contain uppercase letters, lowercase letters, numbers and special characters;
- It must not be disclosed to anyone, no matter how close or trusted the person we want to tell is
- It is recommended not to use personal information when creating a password (eg: parents' names, date of birth, pet's name, etc.);
- Change your password periodically;
- Sign out of your account when you're using a device that's not yours or is being used by someone else.

Do your security updates on time!

- Social media platforms regularly introduce new privacy and security settings. These can be found in your account settings, and it is recommended that you check them regularly;
- Use the two-factor authentication (2FA) option to make sure someone isn't trying to hack your account.

Do not accept friend requests from anyone!

- Accept or send friend requests only from/to people you meet in real life or to public people you are interested in by taking care to follow their official profiles;
- DO NOT FORGET! If you feel attached to certain accounts you can restrict their access to your posts or you can block the account. You also have the option to report accounts or posts for reasons such as: fake account, fake name, posts with inappropriate content, incitement to violence, false information, etc.
- DO NOT click!
- Many attackers use social engineering to gain a person's trust in order to later gain access to information;
- Do not open links and attachments from social media if you are not 100% sure of the source (e.g. websites offering prizes are often intended to steal information);
- If from the chats, a friend seems to be behaving differently (asks a lot of questions, becomes very curious about his personal life, asks for money) there is a possibility that his account has been hacked and an attacker is using it for malicious purposes.

Think twice before posting!

- Social media offers as much an opportunity to create a positive online reputation as a negative one, in addition, even if we "delete" a post, once it has appeared online it cannot be permanently deleted;
- Don't reveal too many personal details on social media! "About Me" fields are optional.
- The boundary between professional and personal life in the online environment
- Do not disclose information about your employer online
- Don't post work photos or negative messages that put the employer in a bad light.
- Think before you post and don't risk your job.

Close old accounts!

- If you have old accounts on social media platforms that you no longer use, or even old accounts on the same platform, try to close them. In this way you create as few links as possible with current accounts being more protected from possible attackers;
- Older accounts or platforms may not be as secure as today's.

Social media poses great risks

- Social networks pose high security and privacy risks due to their centralized architecture, their

huge store of personally identifiable information that any hacker would love to have, and the general ignorance of the population about how to properly use social media. privacy settings to improve their online safety.

- Another very high risk, especially among teenagers, is trusting other people and the type of personal information disclosed online.
- This can be combated through technological means and the enforcement of security policies.
- We should consider information transmitted through social media to be insecure and therefore not transmit sensitive information through social media, thus the primary responsibility to stay safe rests with the USER

Bad social media habits

- Social networks are widely used platforms by users today. We have a wide range of possibilities available.
- Some are more geared towards uploading photos or videos, others towards our opinion and in other cases simply to keep in touch with friends and family. In any case, we are dealing with platforms that have many users around the world.
- This also makes hackers set their sights here. We will talk about these habits that should be changed in social networks if we want to keep our privacy and security.
- There are many types of platforms that we can find on the network that give us the opportunity to send messages to friends or family, commenting on photos, videos ...
- This makes them a very popular environment for both private users and businesses.
- However, this also causes you to have some risk to our security and privacy. Hackers can watch here to carry out their attacks. They can especially take advantage of bad user habits when using these platforms.

Habits that need to be changed

- Privacy and security are very important factors for users.
- However, they are not always present.
- We can be victims of many types of attacks that compromise these two factors.
- We can also make mistakes when using social media and it affects us.

Add any type of contact

- A very common error in social networks is adding any type of contact. This can happen on platforms like Facebook.
- It is possible that what we are adding is a bot rather than a real user.
- You need to know how to differentiate them and avoid adding any type of contact that your invite receives.
- Sometimes bots are designed solely to collect user data. This may compromise our privacy. We need to have a real filter on the contacts we add.
- It is important that we have people among our friends who are not a problem for our security and privacy.

Don't connect with social networks from anywhere

- You often log in through social networks on any site. This is very comfortable, but not the best for privacy.
- Certainly on many occasions we find the possibility to register on a page or to connect to a platform through Facebook or Twitter. We avoid registering on that site and filling out a long form. The problem is that we provide personal data to that website through Facebook. This data / information we share can be used by third parties for advertising purposes.

Do not provide more information than necessary

- It is definitely one of the worst habits that many users have. They enter a lot of personal data, information that is not really necessary, into social networks.
- For example, data such as our phone number, email address, information about where we live ... All this affects our advertising and could be used for bad purposes.
- Don't give more information than is really necessary. In this way we will improve our privacy in the network, and we can even avoid certain security problems.

Spreading fake news

- The problem of fake news is still present today. I can reach them through many means, but without a doubt in social networks they are more than presences.
- As we know, it is fake news that they use as bait and can sometimes even distribute malware.
- It is important to avoid sharing this type of fake news and also to access it when we see it on social media.
- This will improve our security.

We do not protect our privacy

- A final mistake is not properly protecting privacy. For example, we leave our profiles open for anyone to enter.
- We provide information to anyone who might collect it to create a profile for us and even send targeted advertising or perform various attacks that affect our security.

Social engineering from an interdisciplinary perspective

- Due to the technique used by hackers, it is necessary to approach an interdisciplinary perspective such as information technology, psychology, business and ethics.

The discipline of information technology

- Social engineering should be discussed in the context of current information systems and their defence used as a form of risk mitigation.
- Multi-factor authentication is a common and often effective way for organizations to confirm that the person accessing systems should actually have that access

- An additional factor could be the use of a virtual private network (VPN), i.e. authentication to further validate the user.

Psychology discipline

- It is necessary to understand the concept and understand the thoughts and behaviors of both the attacker and the victim.
- The methods are important for social engineering because they are used to bypass protections that may be in place, such as firewalls and systems used to identify intruders.
- It helps to understand employee actions that are one of the main causes of data breaches.

Business perspective

- it is important because social engineering can affect many types of businesses and have implications for how organizations are structured and managed.
- it helps determine the factors that influence social engineering attacks and is beneficial if considered in more specific terms in relation to the following business areas: training and development, documented policies, internal audit procedures, budgets and organizational culture.
- can detect deficiencies in any of the areas that may contribute to attacks.

Ethical perspective

- it is important in the context of social engineering and related research because the idea of manipulating another human being violates many ethical principles.
- helps, in the case of a social engineering event, to treat the victims.

It is important to consider:

- each discipline, providing information on how to understand and interpret the subject, protect against different types of attacks, and understand the impact of social engineering from both a human and organizational perspective.
- that each discipline's interpretation of the subject is useful only when viewed in the context of the other disciplines.

Security techniques

- Equipment inventory
- Inventory of applications and operating systems
- Wireless equipment control
- Network security design
- Limiting and controlling network ports, communication protocols and services
- Protection of perimeter areas
- Physical access to locations
- Controlled use of administrative privileges

- Monitoring and controlling user accounts
- Skills assessment and security training

VPN (Virtual Private Network)

A virtual private network is a secure connection over an insecure network such as the Internet. Virtual means the existence of a unique network, regardless of topology, that is, a group of geographically distributed computers that communicate and can be administered as a single network.

Private means a virtual network with access control. which provides confidentiality, the integrity of messages and authenticates between the users and the computers participating in the communication.

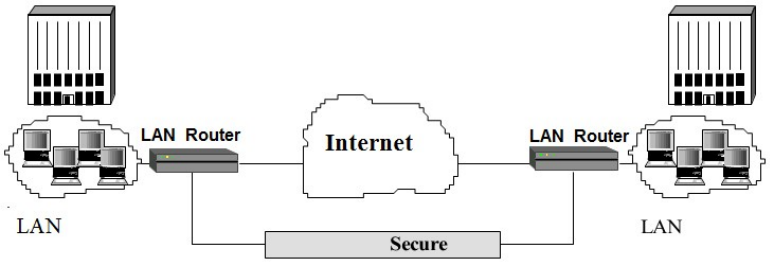

Fig. 2: VPN (Virtual Private Network)

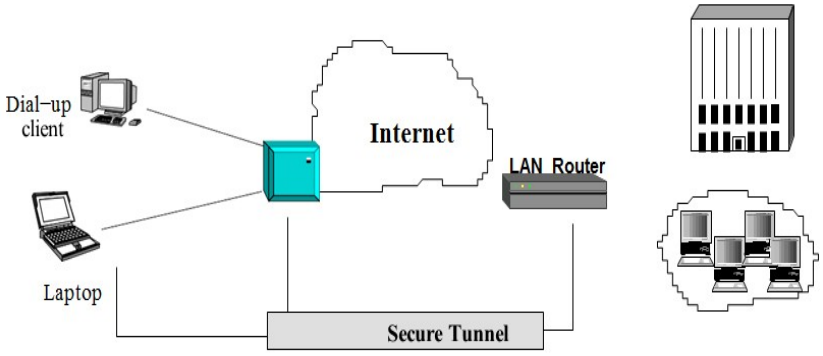

Fig. 3: VPN for remote access

Creating a secure industrial infrastructure

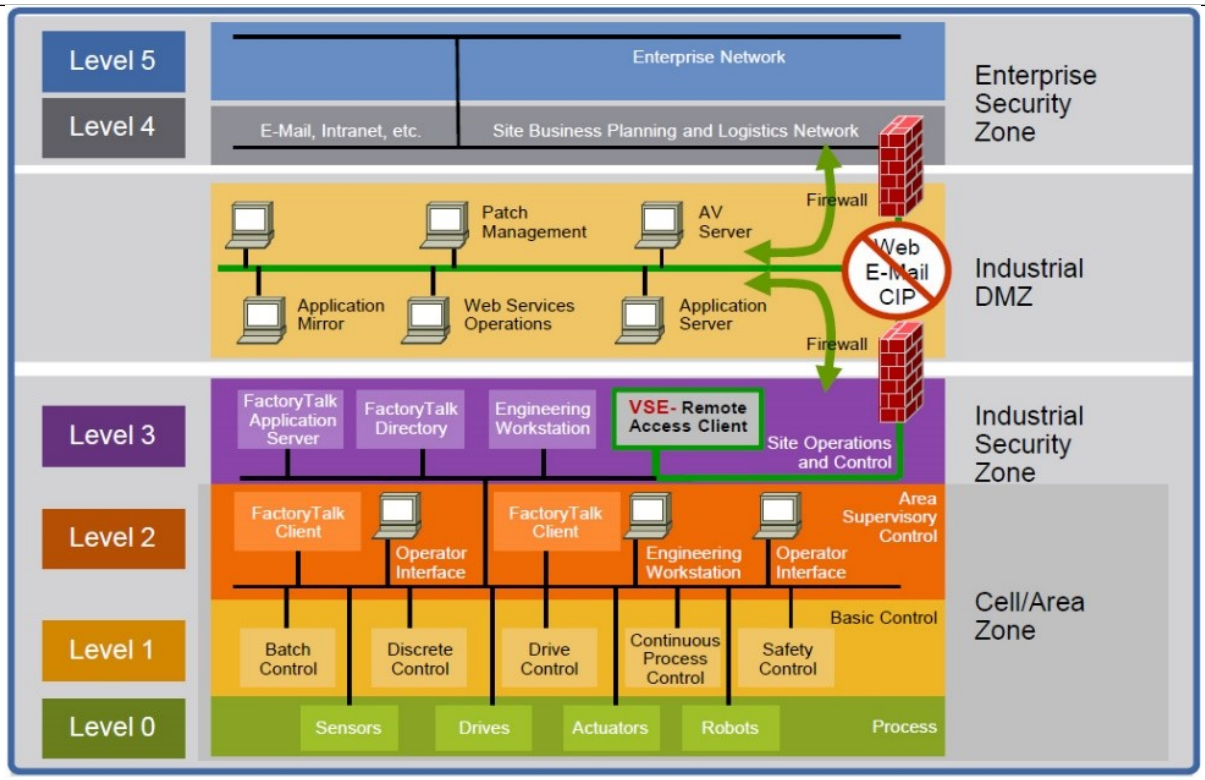

Fig. 4: ISA 95 Logic Model - Industrial Automation and Control System (IACS)

- Defense-in-Depth (DiD) supports this approach. Based on the notion that a single point of protection can and likely will be defeated, DiD security establishes multiple layers of protection through a combination of physical, electronic and procedural safeguards.
- A bank uses multiple security measures—such as video cameras, a guard, and a vault—this helps ensure that threats meet more than one line of defense.
- A security-in-depth approach comprises six main components:

1. Policies and Procedures
2. Physical
3. Network
4. Computer
5. Application
6. The device

Creating a secure industrial infrastructure

- Physical security should limit personnel access not only to areas of a facility, but also to entry points into the physical network infrastructure, such as control panels, cabling, and devices.
- Segmenting plant areas into virtual local area networks (VLANs) is a network-wide security best practice.
- Smaller VLANs are easier to manage and maintain in real-time communications.

- They can help isolate devices from those that have been compromised, which keeps the negative impact within a single VLAN.
- One of the technologies discussed should be an industrial demilitarized zone (IDMZ), which creates a critical protective barrier between the enterprise and industrial areas.
- An IDMZ restricts traffic from traveling directly between the two zones and can help better manage access by enforcing authentication or monitoring traffic for known threats.

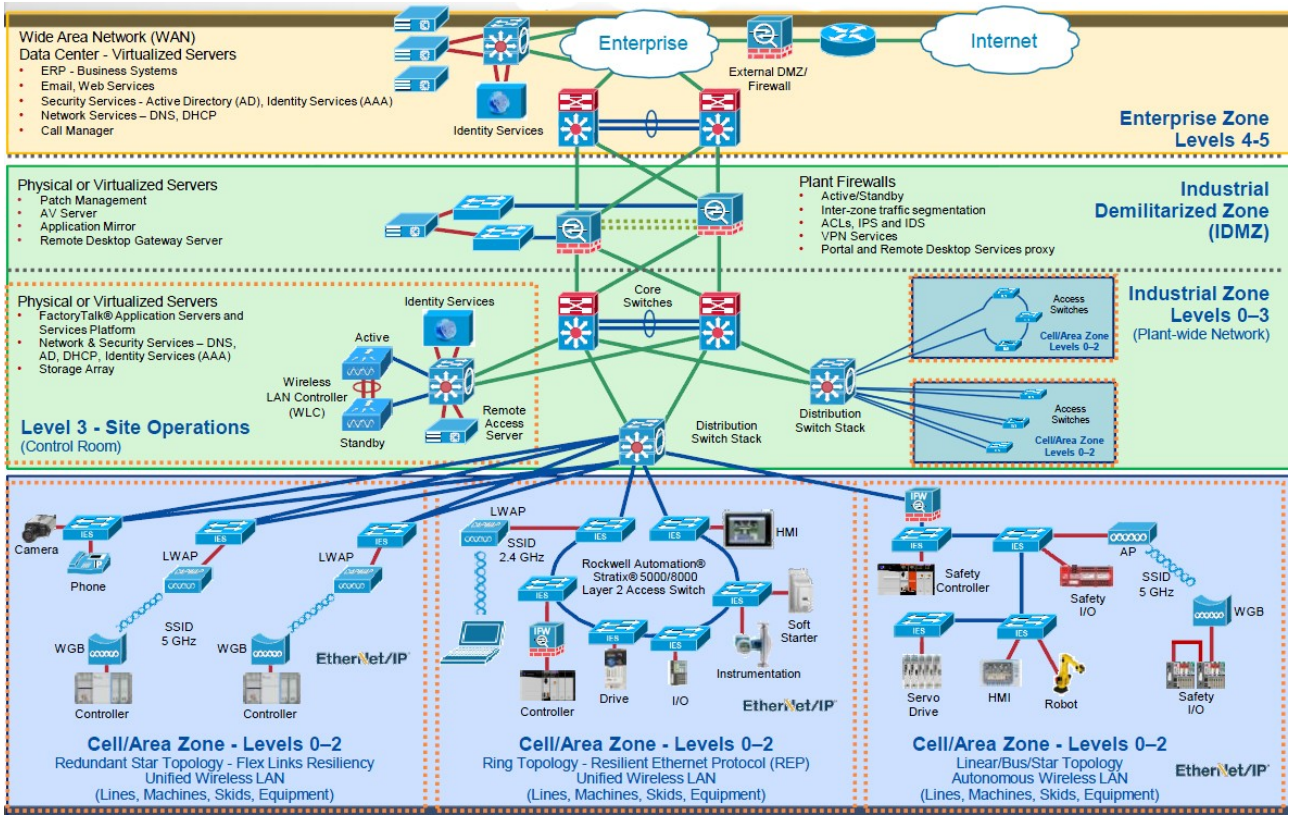

Fig. 5: IDMZ

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. Which are the Risks in Social Networks
2. Measures to have Security and Privacy in Social Networks
3. Which are the main Security techniques in Social Networks

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- Risks in Social Networks
- Security and Privacy in Social Networks
- Security techniques

Attachments *(PowerPoint presentation, handouts, prints, links, video…):*

See attached

References:

Procurement Requirements
URL: Procurement-requirements
URL: https://www.ekransystem.com/en/blog/third-party-providers
Procurement Requirement Determination
URL: https://www.procurementclassroom.com/procurement-requirement-determination/
Security and Privacy in Social Networks
URL: https://www.igi-global.com/chapter/security-privacy-social-networks/14073
Security and Privacy in Social Networks
URL: https://sefcom.asu.edu/publications/security-privacy-social-ic2011.pdf
Privacy and Security in online social media
URL: https://www.geeksforgeeks.org/privacy-and-security-in-online-social-media/
Data Security Techniques and Privacy
URL: https://www.educba.com/data-security-techniques/
What is Security Techniques
URL: Security-concepts-developments-and-future-trends
Most Effective Security Techniques
URL: https://dzone.com/articles/most-effective-security-techniques-part-1
URL: https://panorays.com/blog/what-is-a-third-party-vendor/