Lunch & learn

Consultant Programme

nedap

www.nedapsecurity.com

Content

At Nedap we understand the crucial role a security consultant plays in every project. We understand the vast amount of knowledge required for you to correctly advise your clients on their security needs. From enterprise risk management, crime prevention through architectural design, integrated systems, managing legacy technology migrations as well as regulations, standards, local laws, new trends, cyber security and more. All of this across the multiple disciplines in the world of security, not just access control. It's almost mission impossible.

That is why at Nedap we have created the Consultant Programme which is purposely designed to support consultants in their everyday activities, from specification and design support, updates on new trends and technologies, or general security systems advice. Our group of security professionals have a huge wealth of experience and are here to make your lives easier, so that you can better support your clients.

One of the ways we can help is through our series of Lunch and Learns. These sessions are designed to be delivered during the consultant's lunch break over a sandwich or two, or as times are changing due to Covid-19, they can also be delivered via an online meeting. In the UK you will earn CPD points for you Continuing Professional Development and be issued a certificate so that you can support your learning hours. Nedap are a proud partner of the Security Institute and the CPD points awarded are endorsed by the institute.

Our series of Lunch and Learns are continuously expanding to meet the requirements of consultants today and tomorrow. If there is a subject that you require support on that is not currently in our series, then our experts are on hand and happy to discuss this.
For bookings, please contact your local Nedap representative as this may differ across regions. Alternatively, you can find us at **www.nedapsecurity.com**

Michael Lee
Consultant Program Manager, UK

+44 118 916 6820 (office)
+44 782 789 0531 (mobile)
michael.lee@nedap.com

Introduction to access control

Access-control systems are used in many situations - from a simple office building to a court with extremely stringent security requirements. This involves not only people, but also vehicles and business processes. But what is an access-control system exactly? What are its components? And how do they work? In this lunch & learn session, we provide insight into the capabilities that exist for identifying a person and for opening doors.

What's wrong with keys?

We start by explaining the advantages of using an electronic access control system rather than standard keys. We then discuss the architecture of access control systems and describe each component. You'll get a good understanding of how to create a robust design for a security installation.

Beyond opening doors

You'll also learn about card technologies in this session, and we'll touch upon newer methods like biometry and smartphones. We'll discuss everything that's needed to open doors, and more, electronically – from various card readers to different lock types, including wireless locks. You'll get an insight into the best option for each type of door and will also learn how to ensure your client has choices. This includes up-to-date options for car gates and vehicle identification.

The hidden stuff

We finish by looking at the parts of an access control system that are less visible. We'll discuss how everything at door level is connected to controllers, including any wiring needed, and where to put controllers in a building. Last, but not least, you'll see the role software and servers play in access control systems.

'You'll learn the latest about the basic principles of access control systems.'

Questions are welcome!

Our Lunch & Learn sessions are open to everyone. There's plenty of opportunity to ask questions during and after the presentation, so you can learn more about areas most relevant to you and your latest projects.

Design flexibility and effciency into security specifications

Could changing the way you define specifications for physical security systems improve customer satisfaction? This Lunch & Learn session looks at how specifi cations can influence both the cost and performance of a security system by specifying flexibility and efficiency. You'll get the inside view from a global operating manufacturer on the receiving end of specifications, plus recommendations for improving them.

A challenging situation

As a consultant, you're faced with a variety of requirements and demands from different parties that all need to be addressed in your security specification. At the same time, clients expect they can change or add new requirements at any time, even during the lifetime of the system. We'll help you address this challenging situation by specifying a system that's both flexible and efficient.

What does flexibility and efficiency mean?

Everybody wants a system that's flexible and efficient, but putting this into specifications is easier said than done. We'll discuss concrete technical examples of what determines whether or not a system is flexible, and how you can put this into a specification. Then we'll show how automation and system architecture can increase efficiency. You'll get hands-on tips on how to improve the end user's satisfaction.

'You'll learn how to specify a flexible and efficient system.'

Lowering cost but increasing performance

We'll finish by looking at how security specifications influence not just project costs for systems themselves, but operation and maintenance costs too. We'll also apply McKinsey's model to review how the e□ort put into a security system relates to the performance you can get out of it.

Ask away

After the presentation there'll be plenty of time to ask questions and get more viewpoints during a discussion on the subject.

Escape routes; safe and secure

‘How can you prevent criminals from misusing escape routes in your building’? You want people to be able to leave the building using these routes in case of emergency, but you do not want criminals to use the same routes to get in. In this Lunch & Learn session, we will discuss the standards and requirements applicable to escape routes. We will then take a look at the options available for securing escape doors without compromising peoples’ safety.

Standards and requirements for escape routes

Employees and visitors need to be able to leave a building safely in the event of an emergency. Escape routes must therefore always be kept in order. A number of requirements and European standards have been drawn up for this purpose. In the first part of this session, we will discuss what these standards and requirements are and and give practical examples.

Safe and well secured buildings

Your customers do not just want their buildings to be safe — they also want them to be secure. Doors which cannot be locked due to safety considerations must nevertheless be able to keep criminals out. Otherwise, it becomes all too easy for them to break in or steal items. This is why we provide advice for designing buildings which are both safe and secure, so that you are aware of all the options when advising your customers.

‘A well secured building where escape routes are fully compliant with all standards and requirements — it is perfectly possible with the right equipment!’

Ask away!

In our Lunch & Learn sessions, we want to share our knowledge of the latest technological developments, trends, legislation and regulations in the area of access control. There is also plenty of opportunity to ask questions or discussing situations you encounter in everyday practice. Our Lunch & Learn sessions are a platform for you to ask precisely those questions which will help you in your project!

Integrating biometrics with access control

In the consumer world today, we take the use of biometric technology as standard. Every day millions of people all around the world use their finger or face to unlock their smart devices. The world's largest technology companies introduced biometric technology as the new standard, and the market reacted. But in security, we see something very different. There is still a lack of understanding about how to deploy biometric technology into security systems. Where can we use it most effectively? What are the design considerations? And how exactly does it work?

Why biometrics?

In this lunch and learn session we will take a brief look at the history of access control, and why we may need biometric systems. Sometimes the use of a physical credential is not a viable solution, so what are the options? Many are choosing to use a biometric reader instead of a more traditional card reader, thus negating the requirement a card....or does it? We will explore the different types of biometric systems and the advantages and disadvantages of each.

Biometrics with access control

We will look in detail about how exactly do biometric readers work with access control systems, and what are the considerations when designing such a system. Do you require verification or recognition? Many access control systems will state that they integrate with biometric systems, and vice versa. But what exactly does the word 'integrate' mean? It could simply be a hardwired connection between one system and the other, it could be software communication or it could be both. There is no current standard, so we will help you understand the differences.

'We will show you what are the most important things you need to consider when choosing, whether it's the access control, biometrics or entire solution.'

Choosing the right systems

So for someone who's job it is to choose the right product or to design a system, with all of the variations in the market from one manufacturer to the next, making the right choices can be very complicated. This can sometimes result in the client buying biometric system expecting one thing, but end up with another. We will show you what are the most important things you need to consider when choosing, whether it's the access control, biometrics or entire solution.

Securing the security system

It's widely reported in the media that physical security systems, such as access control, are vulnerable to cyber threats. So what can we do to improve the security of security systems? What should we take into account? And can we ever fully trust them? This Lunch & Learn session discusses security best practices to protect against three known threats to security systems. It considers the influence of people and procedures, as well as technology, on the security of organisations and their systems.

Looking beyond technology

First, we'll look at how the threat landscape is changing: because technology is always evolving, new ways for people to attack an organisation are constantly being developed.

To meet the highest levels of security, it's clear we need to focus on more than just technology. It's vital to take into account procedures too, and the willingness or ability of people to follow them. We'll talk about the interplay between people, procedures and technology when it comes to the security of systems – and how each affects the other.

Protection against common threats

Next, we'll look at three common threats in the access control industry, and recommend technological measures to protect against them. For each, we'll also describe the role that people (the system's users), procedures and technology play in addressing that particular threat.

> 'The technology we implement must be capable of adapting to future threats'

How to be future proof

Finally, we'll look to the future. Because, for a security system that will be in place for at least ten years, taking these measures into account isn't enough. Even though the threats we'll face in the future are unknown, the technology we implement must be capable of adapting to them.

Ask away

After the presentation there'll be plenty of time to ask questions and get more viewpoints during a discussion on the subject.

Usability & Security: a precarious relationship

Where do you stand on usability versus security when it comes to access control? How does one affect the other? And is it possible to maximise both? This Lunch & Learn session looks at the relationship, and conflict, between security systems and their usability. You will not only learn how to increase usability, but how to balance that with the security levels needed.

Interplay

We will begin by looking at the interplay between usability and security. In particular, we will consider the different perspectives from which usability can be viewed:

- **The tasks people need to perform to operate a security system**
  What is the experience like for people using security systems on a daily basis? How easy is it for receptionists to use for them?

- **The automated tasks a security system can perform**
  How can automation not just make things easier but eliminate human error? Can it help to reduce costs?

- **What people need to do to gain access**
  How are people using the building affected by the security procedures they need to follow? What effect can access control have on a visitor's perception of the organisation?

> 'We'll share the measures that increase both usability and security.'

The optimum relationship between usability and security differs with each project. The only way to achieve it is to begin by considering the organisation's needs from the three perspectives above. The next step, of course, is to design a security system to put it into practice. Based on market research in five European countries, 35 years' experience developing security systems and feedback from our customers in 73 countries, we'll share the measures that, from each perspective, increase both usability and security.

Ask away

After the presentation there'll be plenty of time to ask questions and get more viewpoints during a discussion on the subject.

Wired or not to be wired?

This Lunch & Learn session deals with the practice of assigning access control measures to each individual entrance within the building or site. The market offers a variety of access control measures that can be applied. The recent introduction of wireless electromechanical locks that operate online with, or offline from, a central access control system triggers the need to revisit the criteria of where and when to apply them rather than hardwired electronic lock systems.

Setting the scenery

We'll first discuss the trend of mass customised products that due to the internet flood many different markets, and influence modern product & systems design, consumer's behaviour and people's lifestyles. Given this trend, we question the need for access control measures to also be customised. And if this is required, how it needs to be done and specifically what criteria should be followed to provide a set of security measures that are effective in their purpose as well as in cost.

The confrontation

Today's wireless electromechanical locks promise to offer the silver bullet solution for all entrances. They are easier and therefore cheaper to install compared to hardwired electronic lock systems. Why not use them at all entrances?

From the perspective of managing security risks, access control measures play a vital role in preventing persons with ill intentions from inflicting damage to organisations by getting unauthorised access. Not all areas or rooms in a building or site carry equal risk with equal consequences. Is there an ideal set of access measures that can cope with all these different risk profiles or should we take measures proportionate to the risk? This question will be answered by analysing what factors drive risk and how these factors could help you to create a decision model with a hierarchical set of risk levels for the assignment of appropriate measures.

> 'Why a one size fits all approach doesn't work.'

The resolution

Based on that model a bill of recommended access control measures is generated, that helps you to define a consistent set of measures that meet the risk challenges belonging to the individual entrances. At some entrances, risk considerations may prevent you from using wireless electro-mechanical lock solutions. At other entrances, additional criteria should assist you in determining when wireless online or wireless offline solutions are feasible and even preferred over hardwired electronic locks.

The discussion

After the presentation there will be room for questions and discussions.

Zoning and the design of a security system

How to translate a floor plan, specific customer requirements and a risk analysis into a good security system design? Besides making a building secure and meeting the customer's specific requirements, a security system must also stay within budget and be easy to use. At this Lunch & Learn session, we will go into the 4-step zoning model for effective security system design. These 4 steps can be used in any project.

4 clear steps

The 4-step zoning model gives you foundations from which to tackle the zoning of a building in a structured manner. Using a sample project, we will look at how a building is to be secured from the outside inward by dividing the building into zones (areas). We will then look at what security controls would be expedient in each of these zones separately.

From standard to comprehensive security controls
As the security needs increase from one zone to the next, we will go into more comprehensive security controls in greater detail, covering security features such as anti-passback, airlock, manager first, verification and the two-man rule. We will also look at ways to integrate an access control system into a burglar alarm system or CCTV system.

> 'Appropriate security controls are identified for each zone in a building.'

A good design

By following these 4 steps in designing security controls, you will make sure you will not underdo it and compromise the building's security. But at the same time, it will make sure you do not overdo it either, allowing you to keep costs under control and ensure a user-friendly building.

Ask away

After the presentation there'll be plenty of time to ask questions and get more viewpoints during a discussion on the subject.

nedap

www.nedapsecurity.com