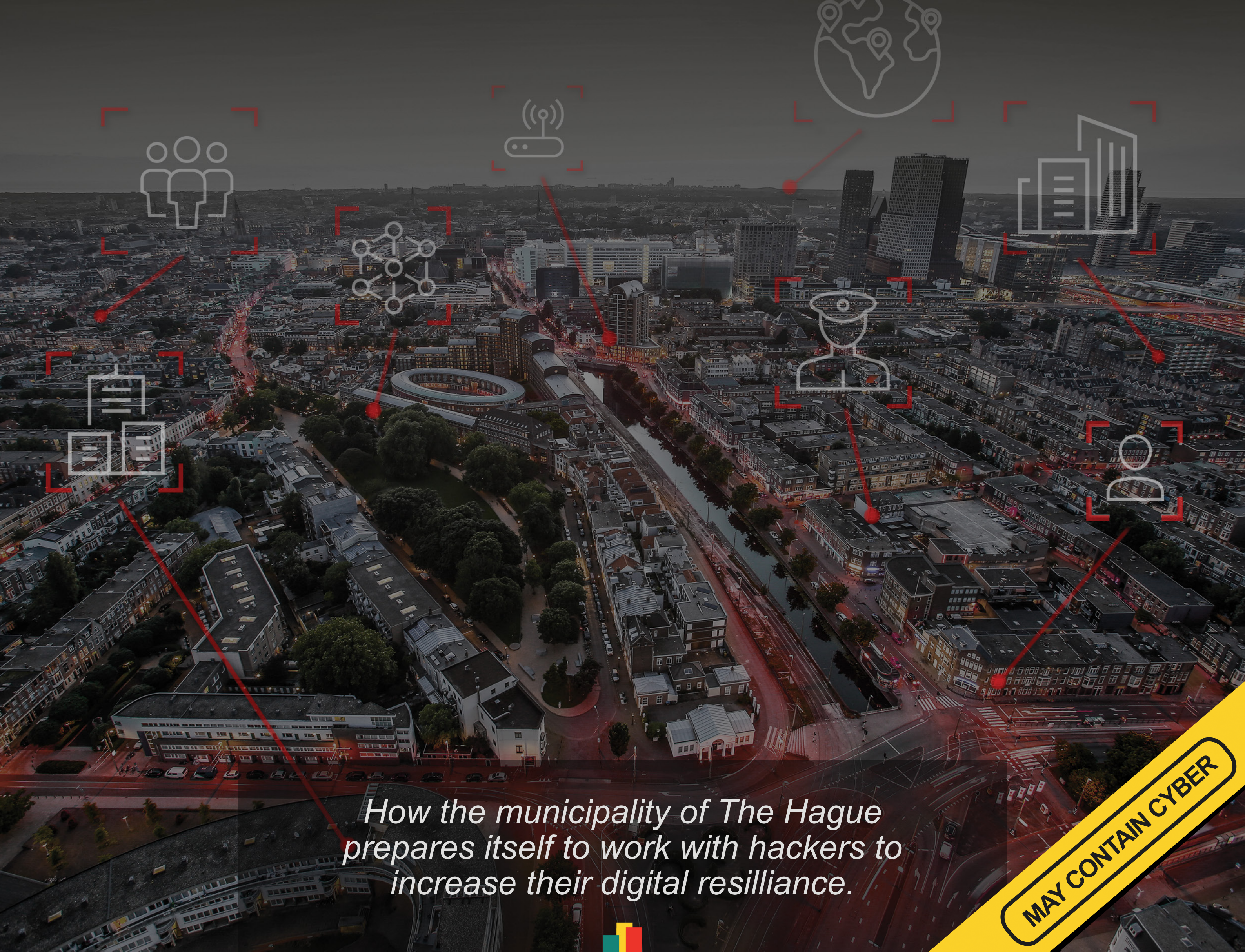
CYBERSPRINT
BREAKTHROUGH SECURITY

The Hague

E-GUIDE

HOW TO HACK A CITY / COMPANY / ORGANISATION / COUNTRY / ETC.



How the municipality of The Hague prepares itself to work with hackers to increase their digital resilliance.

MAY CONTAIN CYBER

TABLE OF CONTENTS

PREFACE

Since 2017, the Municipality of The Hague organises the annual hackathon: ‘Hâck The Hague’, as (an important) part of its policy to promote digital resilience, together with cybersecurity company Cybersprint. An open, transparent event, which is held in the Atrium of city Hall (or online, as was the case in 2021) and during which hackers are challenged to test the security of the computer systems of the municipality and its suppliers, in a controlled environment.

Following the event’s success, both the city and Cybersprint have been approached by other municipalities and the business community about how to organise such an event. The result is this document, which contains an overview of the acquired experiences, to be shared with the largest possible group of Chief Information Security Officers, ICT and Security Managers and policy-makers. They can use it as a guideline to host their own hackathon but it also informs them about the measures they need to take to prioritise, monitor and resolve any vulnerabilities in their websites and systems.

This e-guide broadly describes what you need to do to prepare your organisation to continuously improve cybersecurity and how you can involve hackers in this process. Yes, indeed: ‘how you can work with hackers to increase your digital resilience’. For many people, the word ‘hacker’ has a negative connotation which is entirely understandable given all the media coverage of digital fraud and cyberattacks. That is why it is important to understand the difference between ethical hackers and black hat hackers, with criminal intentions. Ethical hackers are socially engaged people, who use their knowledge, insight and experience, becoming an indispensable link in the chain that is involved in securing systems and information in more and better ways. Any time we refer to hackers in this e-guide, we are of course referring to ethical hackers.

Given that cybersecurity is related to so many different subjects, this document is far from comprehensive. We recommend checking beforehand whether a hackathon is compliant with the local regulations and legislation that your organisation is subject to. Topics that you may also want to review during your preparation, but which are not covered in this e-guide, include:

- Dealing with internal policy, decision-making, and obtaining a mandate (you can use this e-guide as a conversation starter!).
- Establishing the organisation’s maturity and preparedness to take a cybersecurity risk.
- Determining what is needed to achieve and measure these objectives. This includes but is not limited to financial resources, capacity, knowledge, own staff/contractors, etc. We recommend partnerships with existing security and chain partners and your peers.

Once you have completed this preparatory process, you can make a well-considered choice whether a hackathon is the right solution for your organisation and how such an event will contribute to improving cybersecurity. Compared with the preliminary work that is needed to ensure that cybersecurity is an integral part of your organisation, hosting a hackathon is child’s play. At the same time, such an event requires seamless organisation and coordination. Always remember that if the outcome is less than perfect, the hackathon can soon become a source of negative publicity, among hackers and the public. In extreme cases, it may even result in data leaks which nobody wants. If you conclude that a hackathon is a good addition to the overall effort and measures that your organisation has put in place to guarantee cybersecurity, you can use the scenario in this e-guide to organise your own hackathon.

Thanking all the people who contributed to successful previous editions of Hâck The Hague and indirectly to this e-guide is impossible. We do however want to thank Peter van Eijk in particular, for sharing his knowledge and expertise as Information Security Manager at the Municipality of The Hague and all those people who made a direct contribution to the content of this e-guide (in alphabetical order, by first name):

Chantal Stekelenburg (Head of Operations - Zerocopter), *Chris van ’t Hof* (Host, Researcher, Author and IT Event Organiser), *Daan Rijnders* (Lead Cyber Secure - Municipality of The Hague), *Edwin van Andel* (CEO - Zerocopter), *Frank Jan Uittenbogaart* (CEO/Product Development Manager - DG Groep), *Jonathan*

Bouman (GP and Hacker), *Michel Slootweg* (Information Security Officer - Municipality of The Hague), *René Kroes* (Product Owner, I-REAL), *Saskia Bruines* (Alderman for Economy, International Affairs and Services - Municipality of The Hague), *Vincent Thiele* (CISO - Cybersprint), *Wietse Boonstra* (Security Researcher, Bug bounty hunter and Hacker).

We hope this e-guide contributes to increasing cybersecurity in The Netherlands and beyond. We welcome any questions or remarks that contribute to the further development of our joint insights into cybersecurity.

Jeroen Schipper
CISO Municipality of The Hague

Pieter Jansen
CEO Cybersprint

The Hague, November 2021

EXECUTIVE SUMMARY

Internal and external stakeholders
Cybersecurity is not something you can afford to work on from the comfort of your ivory tower. There are too many different internal and external stakeholders involved. And each plays a role in the digital resilience of a government organisation or commercial company. Personal interests, own responsibilities and conditions must be fulfilled before these people can make a positive contribution to the cybersecurity objectives that were set. In a municipal context, you must take into account the mayor and aldermen, other decision-makers,and the employees of ICT and security departments, as well as directors and the users of these systems. In terms of external stakeholders, you should ask yourself a number of critical questions:

- To which extent are clients/citizens aware of the importance of the security of the systems in which their data are stored, processed and shared with third parties? What do they expect from your organisation in this respect?
- What about the suppliers of systems and services that you use?
- How do you involve hackers in the testing and improvement of your cybersecurity in the right way?

In Chapter 1, we provide an insight into the various aspects that are important for internal and external stakeholders.

Organisational readiness
Preparing an organisation to take steps to improve its cybersecurity involves several aspects. The (re-)organisation of the security and ICT organisation,

ensuring that you have sufficient qualified personnel in your own organisation, potentially supplemented with external expertise in the form of contractors or strategic partners. Another important factor is the way in which your organisation responds to future incidents. Processes that have been developed and describe which actions are required in case of a future (or ongoing) attack or when a vulnerability in your system is reported. Another element is the evaluation, replacement and procurement of the required systems and infrastructure. Systems that help you map your organisation's digital footprint and the attack surface area, coordinating tooling that provides an overview, insight and efficiency and bug bounty platforms which you can use to deploy hackers' expertise. Reaching out to groups of hackers that are either in direct contact with your organisation or regularly check your systems for possible vulnerabilities through an intermediary. In all of the above cases, good communication with internal and external stakeholders is crucial.

Chapter 2 describes the levers for preparing your organisation for the implementation of an adequate cybersecurity policy.

Hackfest

As soon cybersecurity is engrained in every aspect and level of your organisation, you can consider organising a hackathon. Hackers compete against each other in a controlled setting to detect possible vulnerabilities in your websites and systems. Besides seriously considering the added value of such an event for your organisation, you must also make decisions about the following:

- What is a good time for this event?
- Will you organise a live or an online event?
- How many hackers do you want to invite?
- Professional hackers or also students?
- Will you let them hack your own systems or also your suppliers' systems?

Most of your attention should be directed at prioritising, monitoring and resolving the vulnerabilities that were detected during the event. The learnings from this event are the main ingredient for achieving growth in terms of cybersecurity.

These and other points will be discussed in more detail in Chapter 3. You can find a script for a hackathon in Annex 1.

Conclusion

The desire to digitalise is continually increasing and is inextricably linked with attention to cybersecurity. The more processes are digitalised, the more important it is to ensure that they can take place safely. Important systems become unreliable and thus unusable without adequate information security. Setting up cybersecurity processes and systems and working with hackers takes up a lot of your time and energy but the results are always positive. Good digital resilience is invaluable because it can prevent costly repairs, image damage, loss of clients and more. By actively involving hackers in your cybersecurity policy, you can always stay one step ahead of cybercriminals.

HÂCK THE HAGUE, ALWAYS SUSPENSEFUL, BUT EXTREMELY VALUABLE

“Society is digitalising and as a city we must keep in step with this evolution. Inhabitants can expect the same speed, service and innovation from their city. In an international city of peace and justice like The Hague, security is a preliminary condition, which is why the city prioritises well-secured ICT systems. That is why The Hague invites large numbers of hackers to hack its systems every year, during its annual Hâck the Hague hackathon. Suspenseful at times, but the event also yields lots of valuable insights. Every year, Hâck the Hague helps to raise awareness, in and outside of the city, attracting a large crowd and the media. Which is good, because information security is incredibly important. National and international hackers participate in this competition during which they must try to circumvent the security systems in place.

Good preparation and clear rules

Hâck The Hague yields other insights than a conventional security test. It also requires a good preparation and clear rules to avoid unwanted situations. That is why The Hague works closely with several experts, such as Cybersprint, one of the partners of the The Hague Security Delta. As an organisation, you must also be able to assess and close any security breach that are identified during the hackathon. So you can see how vital it is that your organisation is prepared. This includes your people, processes and supporting technology.

The importance of cybersecurity
As a city, we find that an event such as Hâck The Hague increases our understanding of how systems are secured. Other eyes take a fresh look at our city’s ICT systems. But there’s more. The competition is also designed to interest students in a career in cybersecurity. This is curcial because the demand for cybersecurity specialists will only increase in the years to come. An organisation can always be hacked. You need to prepare for this. You must also develop scenarios for a cybercrisis. You also need to organise regular cybercrisis management exercises - at all levels - including in and outside of the organisation.

All too often, cybersecurity is seen as something that ‘IT’ will take care of. In reality, this issue deserves attention from and should be a concern at every administrative level. Without this awareness, organisations are incapable of structurally improving their cybersecurity.

Cities and municipalities are increasingly focussing on cybersecurity. In the physical world, a municipality’s competences are easily defined. But the situation is less clear-cut in the digital world. That is why we also discuss this topic at a national level, within the Association of Netherlands Municipalities. We have grouped all our knowledge and experience on cybersecurity and Hâck the Hague in this e-guide. I'm very proud of the result: it shows that The Hague leads by example when it comes to cybersecurity. I really hope that this will inspire and motivate other municipalities and organisations to take the next step.”

Saskia Bruines
Alderman for Economy, International Affairs and Services, Municipality of The Hague

CHAPTER 1
INTERNAL AND EXTERNAL STAKEHOLDERS

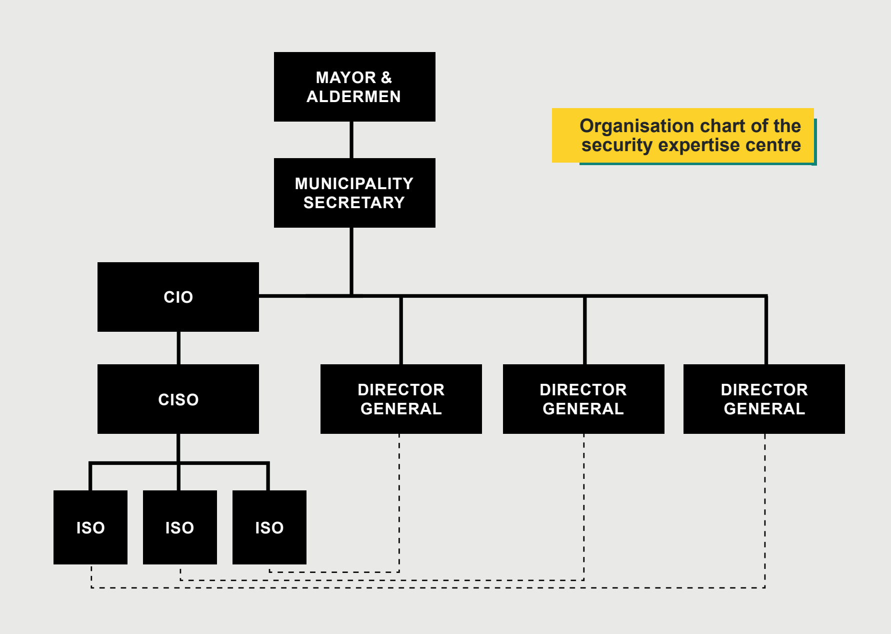
1.1 INTERNAL STAKEHOLDERS

Directors

Tackling the digital resilience of a governmental body or company essentially means not being afraid of being caught with your trousers down. On the one hand, because you are less knowledgeable about this specific area of expertise and are therefore forced to rely on others, within or outside of your organisation. On the other hand, realising that the security of your products or services leaves much to be desired and that a substantial investment is needed to improve this can be quite worrying. Strong persuasiveness and good arguments are indispensable to convince management and/or the mayor and aldermen to take the initiative to invite hackers to break into systems. After all, we are naturally inclined to not disclose bad news. When it comes to cybersecurity the rule of thumb is: the more open and transparent your approach, the better the result.

The municipal objectives that were set by the Municipality of The Hague state that careful handling of the city’s information is an important preliminary condition for the further digitalisation of services. Exemplary behaviour and leadership are crucial to achieve this. To get everyone, at every level of the organisation, on board, you must highlight how important information security is in everything you do as this will influence the behaviour of others and they will act accordingly.

The management of the municipality's administration provides support for and oversees information security. In this context, it also assesses the importance of the various aspects of this information for the city, the risks that the city runs and which of these risks are unacceptably high. This is then used to determine which actions must be taken in terms of information security and to monitor the progress of the roll-out of these actions.


Organisation chart of the security expertise centre

Information security is organised at the strategic, tactical and operational level. And all these levels seamlessly align with each other and the organisation's other processes. The Mayor and Aldermen are responsible for administrative management within the Municipality of The Hague. The city's municipal secretary is responsible for day-to-day implementation. The responsibility for the organisation of information security has been delegated to the Chief Information Security Officer (CISO) by the Municipal secretary, by way of the Chief Information Officer (CIO). The line management of each service is responsible for implementing the information security policy under the supervision of the Director General (Algemeen Directeur, AD). The Information Security Officer (ISO) assigned to the AD acts as an advisor to the AD and the sectoral directors.

To effectively incorporate information security into the organisation, attention must be paid to:

- Processes
- Culture, attitude and behaviour
- Organisational roles, responsibilities and competences

Managers of the ICT and security departments

Chief Information Security Officer (CISO)

The CISO is responsible for all information security (resource) and information security (purpose) matters within a municipality or company and plays a central role. Defining policy standards; analysing possible applications of new developments such as the Internet of Things; determining how to deal with changes in legislation such as the Government Information Security Baseline (Baseline Informatiebeveiliging Overheid or BIO) and the GDPR. Jeroen Schipper, CISO at the Municipality of The Hague, who helped draft this e-guide and who also holds ultimate responsibility for Hâck The Hague, explains his responsibilities and the conditions for making an optimum contribution to cybersecurity as a chief information security officer.

(Chief) Information Security Officer

- independent role
- control and advise
- basic ICT knowledge
- from technical issue to impact on the organisation
- relationship of high trust

Jeroen: "As CISO you have to provide independent advice on information security. You check information security measures and make recommendations. The various directors are responsible for the process and for the underlying information systems. They ultimately decide whether or not to adopt a recommendation and they bear the consequences of this decision. At the Municipality of The Hague, I am responsible, among others, for the city-wide programme on information security. This includes raising awareness of cybersecurity, consultations with various stakeholders within and outside the city's administration, and regular reporting to submit decisions to the city's Mayor and Aldermen.

A major challenge in any information security policy is to ensure that the various responsibilities are clear and that these are also enshrined in policies. In addition, support, a mandate and responsibility from management are a preliminary condition for an adequate response in crisis situations.

> "As CISO of the Municipality of The Hague, I consider Hâck The Hague to be the equivalent of an annual evaluation. When it comes to digital safety and security, you can develop policies until you're blue in the face. But it's only when you organise an event like this, that you will know in practice whether we've done our job properly."
>
> *Jeroen Schipper*
> *CISO Municipality of The Hague*

As CISO and ISO, you need to have a basic working knowledge of ICT to be able to understand the potential impact of technical issues on the organisation. Communication skills are also very important, as is a good relationship of trust with, in our case, the various directors. Finally, you must also intervene in or dare to shut down systems in the event of a calamity, without consulting the organisation, and have good arguments to do so."

Information Security Manager

Peter van Eijk is Information Security Manager at the Municipality of The Hague and plays an important part in the achievement of the city's cybersecurity ambitions. Peter: "Every city has a different cybersecurity risk profile as well as a different dynamic. Digitalisation in cities and municipalities means digitalising the city's internal systems as well as the city as a whole. But this far-reaching digitalisation also increases cybersecurity risks. Our city pays a lot of attention to ways of increasing our resilience. It is not enough to focus on our physical security. We want to limit elusive digital risks by providing an insight into, analysing, prioritising and mitigating them as quickly as possible or, better yet, resolving them completely. Good control systems, good communication and a good relationship of trust with the people you have to interact with are the basic requirements for this.

> "Being in control doesn't mean you have to fix every vulnerability right away. It's about having insight into the vulnerabilities and their possible impact, so that you can make the right decision about whether you need to tackle something now or later."
>
> *Peter van Eijk*
> *Information Security Manager - Municipality of The Hague*

In my role I provide direction and guidance to the ICT Security department at strategic and tactical level, with the aim of achieving tactical objectives. Together with my team, I provide the technical content, advise C-level management and contribute to the development and updates of the Municipality of The Hague's information security strategy and policy plans. As a manager and employee of the security department, you must have a great sense of responsibility, be committed and interested in information security. Don't even bother working in this field if you have a 9 to 5 mentality.

My advice is: think big, but start small. Start with a limited scope: how are the internal processes running, are all your assets registered? See what works and what doesn't and slowly expand things. You can scan the whole world with the technology that is currently available. Unfortunately, this yields so much information that you won’t know where to start and what to do. Involve employees in everything you do. This includes IT professionals and people from within the organisation. They must work to resolve the vulnerabilities. The faster they take steps, the less they will have to resolve. By providing an insight into the positive effects of our efforts, we hope to eventually get people to think along and tackle risks before they become problems.”

Service directors and system users

Good and safe digital services are and will remain an important point for attention. This is the responsibility of the directors and managers of essential departments such as IT and Security, as well as of all the employees of an organisation or company. Within a municipality, directors and system users are a crucial link in the proper and safe handling of information, whether their own or that of third parties. Safeguarding cybersecurity within the organisation is very important. To be able to fix the vulnerabilities that are detected, you need to know who is responsible for the various applications and websites. Unfortunately this is not always clear. And once the owner has been identified, convincing these people to take action or creating a sense of internal urgency to push through an upgrade can be challenging.

The role of the directors within the municipality is described in more detail under the heading 'administrators', but ultimately all employees must have the right mindset when it comes to cybersecurity. Attitudes and behaviours with regard to cybersecurity will therefore have to be regularly influenced by means of awareness campaigns and training. Making and keeping those involved aware of the importance of information security ensures that they can play their own part in this. This promotes the right behaviour and creates a culture in which people actually dare to hold each other accountable for behaviour. At the Municipality of The Hague, the CISO organises these campaigns and training programmes. Ultimately, however, it is each manager’s responsibility to ensure that all his or her employees take this seriously and participate in this. Given the overlap with the subject of privacy/data protection that falls under the responsibility of the data protection officer, awareness training about this and information security is often organised simultaneously. Besides permanent and compulsory training, the CISO and ISOs also organise events and develop publications to ensure continuous attention to this subject.

1.2 EXTERNAL STAKEHOLDERS

Citizens

If we look at the environment in which a Dutch municipality operates, citizens are their first and most important external stakeholder. They are the main customers of these municipalities. It is in their interest that the often sensitive information that is shared with various municipal counters is securely processed and stored. In addition, they are also responsible themselves when it comes to certain aspects of cybersecurity. But what do a municipality's citizens actually know about cybersecurity? And what do they expect from a municipality in this regard? We asked Daan Rijnders, Lead (Quartermaster) Cyber Secure at the Municipality of The Hague.

Daan: "Society seems to have woken up to the importance of cybersecurity. Which is a good thing and important. However, the terminology, as for example used in the media, is very diverse. Cybersecurity, cybercrime, cyber resilience and all kinds of incidents such as ransomware, phishing, DDoS attacks and malware... The use of all these terms, which each have a different angle and target group, only compound this. The English terms also often make everything sound scarier and more complicated. Consequently, people sometimes mistakenly believe that they can't do much in terms of digital security or that they have no chance of becoming a victim of cybercrime.

Fortunately, there are several excellent national initiatives, that were designed to better inform citizens and businesses, such as Alert Online, veiliginternetten.nl and hackhelpdesk.nl. In The Hague, we have developed the 'Digitaal Veilig in de Wijk' (Digital Security in the Community) together with the police force and locals, to increase digital resilience in communities. Citizens and entrepreneurs are trained by us and volunteer as Digital Ambassadors to raise their neighbours' awareness of cybersecurity risks. In recent years, Hâck The Hague has also contributed to raising awareness of cybersecurity among citizens and businesses in our city. While digital security is often difficult to explain, it becomes easier to explain when a few hundred hackers are working live in the Atrium in city Hall while citizens queue to pick up their passport. This is the conversation starter we need."

Suppliers

As with citizens, the knowledge level of suppliers of systems and applications is also different. They are an important part of the (digital) ecosystem of a municipality or company which is why you need to involve them in activities and initiatives to improve your cybersecurity. Michel Slootweg, an ISO at the Municipality of The Hague, is the supplier contact at Hâck The Hague, helping them prepare for their participation in the event.

Michel: "As a city, we understand the suspense suppliers that participate for the first time in Hâck The Hague must feel when they open up their systems to hackers. But experience has shown that the insights that emerge during this competition are very relevant to them. For many companies, they event are a prelude to an (even) better security of their systems and websites. As a city, we are also working on improving the guidance we provide to suppliers each year. We do this, among others, by sharing information and making tools available that suppliers can use to already scan the environments that will be tested for free prior to the hacking event. In this way, they ensure that vulnerabilities that are easy to fix are already resolved before the participating hackers launch their attack on their systems."

So what's it like to participate in Hâck The Hague as a supplier of the Municipality of The Hague? Two companies that have already participated in one or several iterations of this hackathon are willing to share their experiences.

DG Groep:
Data security is now fully guaranteed in our business processes
In 2019, DG Groep participated in Hâck The Hague with its GISIB online application. GISIB online is used to register, inspect and manage all government assets or capital goods, including roads and lampposts as well as grasslands, forests, river banks and reeds. A municipality strives to provide the highest possible product quality to its citizens and GISIB online helps them achieve this. Frank Jan Uittenbogaart, the company's CEO and product development manager, has the following to say on the importance of cybersecurity and the benefits of participating in Hâck The Hague.

Frank Jan: "Information security is a hot topic, and rightly so. These days, we all receive spam and spoofing attacks and strange e-mails from banks that turn out not to be banks. Our own system, GISIB online, contains a large amount of data that needs to be secured against unauthorised use even though 80-90% of this data are publicly available. As an ICT supplier you must remember that our ICT will be useless in 20 years' time without adequate information security. If important systems become unreliable because they are regularly unavailable or do not do what they are supposed to do, they are no longer useful to us. Hâck The Hague is a unique event in The Netherlands, with an important educational aspect. We have also used it to raise awareness of cybersecurity within our company.

Our first participation in Hâck The Hague in 2019 was quite exciting. In effect, you are consciously subjecting your own software to 'torture'. Obviously, we had protected our system to the best of our knowledge, but you can never be sure that this is sufficient when more than 100 hackers are let loose on your systems. Given that data security is not our expertise, we called in external help in the run-up to the event, to review everything one more time. A number of things were uncovered during Hâck The Hague, including security headers on the website that were not completely secure, paving the way for potential data leaks. This was fairly easy to resolve and it was done on the spot. Another vulnerability was found in the software itself and was immediately passed on to the development team, which quickly released a patch to solve this problem. We talked to the hacker who brought the problem to light and he checked the patch on his own initiative to see whether the solution was indeed sufficient.

Soon after our participation in Hâck The Hague in 2019, we participated in a tender. One of the requirements was ISO 27001/2 certification. At the time, we were really happy that we had participated in Hâck The Hague and were already working hard towards improving data security. Essentially this was a prelude. We now perform periodic standard checks of our own business operations and the quality of our software development. Since then, data security has also become an

SUPPLY CHAIN HACKS, A JOINT RESPONSIBILITY

You may associate 'supply chain' with logistics and you wouldn't be wrong. But lately, it's also become a hot topic in the cybersecurity community. The most recent impactful hacks took place in the ICT supply chain. Vincent Thiele, CISO at Cybersprint, explains what supply chain hacks entail and why this requires optimum digital security and collaboration with the largest possible group of parties that you collaborate with.

What is it?

Vincent: "A traditional supply chain consists of all the links needed to get a product from raw material to consumer. ICT has its own supply chain, namely everything that is needed to offer a good ICT service. Whether this concerns a municipality or a commercial company, in both cases all kinds of suppliers are involved in providing services to citizens or customers. Think, for example, of mail servers or software programmes for handling a (customer) question. During a supply chain hack, criminals access the system through one of these gateways, after which they can paralyse large parts of these systems or take them hostage (ransomware).

Supply chain hacks are a relatively new phenomenon. To date many questions still remain unanswered. In any event, it is important to bear in mind that there are three different types of ICT supply chains, each with their own risks:

- In a hardware supply chain hack, for example, elements can be introduced into hardware products of others using chips from a specific supplier, with all kinds of unwanted consequences.
- Software supply chain hacks can be caused by the smallest piece of software you receive from a third party, which is secretly included in a software update from that party. This allows the developers of this insignificant piece of software to gain access to various systems within your organisation, as was the case recently with the incidents in Citrix, SolarWinds and Microsoft Exchange.
- An infrastructure supply chain hack is done through channels that IT service providers use to perform service updates to your organisation's infrastructure.

We have discussed the various types of supply chain hacks in more detail in an editorial on this topic, including the solutions to these risks."

Who is at risk?

"If you are of the opinion that your ICT supply chain is too limited to run any risk, then unfortunately I'm sorry to inform you that you're very wrong. Any organisation that purchases software, hardware or IT services from third parties, whether for its own use or for incorporation in its own products, is potentially setting itself up as the victim of a supply chain hack. And no organisation develops 100% of their hardware and software in-house. The mere download of a publicly available plug-in to monitor the performance of your website can be the Trojan horse that unknowingly and inadvertently gives criminals access to the heart of your organisation.

And many of the organisations whose systems and/or software were infected are large and leading organisations. Recent examples of high-impact supply chain hacks include Kaseya, a service provider that provides security services to several companies, and SolarWinds, a widely-used IT monitoring and management tool."

What can you do?

"Supply chain attacks seem to be increasingly common and at the moment there is no uniform solution available. It is vital that you know which hardware and software your organisation uses in this context. You must be aware of the risks that this can entail and be able to act immediately when something actually goes wrong. If one of your third parties is infected, every second counts. If you have to start by looking for instances where you use this software, you are simply losing time and are unable to start working on a solution.

Make sure that the suppliers you work with pursue the same level of security as you do. Yes, I know it's a tired cliché, but your cybersecurity is only as strong as its weakest link. Remember to include agreements about the security measures to be taken unambiguously and transparently in your purchasing and/or connection conditions. Don't forget to actively monitor compliance with these agreements so that it is clear that this is not a formality.

At Cybersprint we closely monitor our environment and that of our customers, keeping close tabs on the potential impact of third parties. We see this as an opportunity for collaboration with partners and suppliers. When we detect a vulnerability in a supplier's attack surface, we discuss this with the supplier to resolve the issue. This is beneficial both parties.

The Municipality of The Hague also does this. Hâck the Hague is a small but good example of their approach. The digital safety of the systems of the city and of a large number of its suppliers is tested. By involving third parties in the event, the scope of the research - and its positive impact - is several times greater. This is just one of many ways in which we can help each other achieve a higher security level".

integral part of our business processes. My advice to all the suppliers of the Municipality of The Hague is to participate in Hâck The Hague. By collaborating with hackers, we raise the bar for each other. They help us, as suppliers, by investigating the ins and outs and identify possible vulnerabilities before malicious parties do this. Are you not sufficiently knowledgeable about data security? Then hire an expert to advise you. But don't let this deter you from participating in Hâck The Hague because it is a very valuable experience."

I-REAL: Hâck The Hague helped us take our cybersecurity to the next level

I-REAL creates the Internet of Things for the public sector by giving administrators access to objects that contribute to the drainage of water. The Municipality of The Hague uses their product, I-REALM2M, to monitor, control and manage elements in the water chain and public infrastructure. René Kroes, Product Owner at I-REAL, explains why Hâck The Hague is a welcome addition to the measures they have already taken to improve the security of their software.

René: "Our software helps municipalities to manage their water and public infrastructure and to control objects such as fountains, bridges and moveable fences. So you can see how worrisome it would be if someone hacks into our software and takes control of all of these things. That is why cybersecurity has always been an important area of focus within our company. In addition to our participation in Hâck The Hague, we also regularly conduct pentests and other activities to keep our ISO certification up to date. Municipalities expect the solution that we supply to them to be foolproof and to date this has always been the case.

Our software is under development. We always weigh the degree of accessibility of the software against the maintenance of the necessary security levels. Hâck The Hague is just one of many ways to test whether our approach is successful. We prefer to have a participant in this event discover a vulnerability in one of our products rather than unknowingly leaving the door open to strangers with bad intentions. Obviously, it's never fun when someone identifies a major bug in your system, but at least it gives you an opportunity to resolve the issue. By participating in Hâck The Hague, you show that you take cybersecurity seriously and that you work with experts in this field to improve your products."

Hackers

Many people still equate the term 'hacker' with shady characters who engage in criminal activities on the fringes of society. But they are wrong. These hackers report more or less impactful vulnerabilities in time to product owners so they can take measures before someone abuses them. In many cases hackers also earn a bonus when they report vulnerabilities. But many of them do it because they feel that they can make a concrete contribution to improving cybersecurity.

Criminal hackers continuously try to break into organisations such as the Municipality of The Hague. When a new city system is connected to the internet, it generally takes just 2 minutes before the first attack is launched. These are not the kind of hackers you and we want to work with. Ethical hackers, on the other hand, are 'a different species' altogether: they attempt to get into systems with the aim of making applications and websites more secure. They abide by the rules and report the vulnerabilities they detected to the relevant organisation to prevent them from being misused by people with malicious intent. But why do these hackers participate in a competition and which responsibilities do they think they have in the cybersecurity context? We asked two active hackers: Jonathan Bouman and Wietse Boonstra.

What is the importance of cybersecurity in your opinion and are companies doing enough to guarantee it?

Jonathan: "I work as a general practitioner. My work is based on a relationship of trust between the patient and doctor. I can only do my job if my patient trusts me. At the same time, I have to be able to count on the security of the computer in which I record everything. A principle that applies to healthcare as a whole. I find digital security very important, which is why I'm happy to contribute. In principle, all systems have major or minor vulnerabilities. Leaks are not that problematic, but if a vulnerability is detected, it must be resolved quickly. The only way to do that is to share knowledge, resolve the issue and make sure everything is safe again as soon as possible. Together you are stronger, even if you want to take a stand against cybercrime. Share knowledge, let the community work for you as a team, promote cross-fertilisation. Once your employees have become acquainted with hackers and engage with them openly and transparently, they will find it easier to reach out to each other when necessary.”

Wietse: “Nowadays everything is digital so this is definitely something you need to take into account. As a company, but also as a private individual. If your password to your mailbox is not secure and you have sent a copy of your ID by e-mail, for example, a criminal can easily access this and impersonate you online without any problems. Just think of the hack at the municipality of Hof van Twente, which was entirely due to a password that was too simple. Obviously I know how this can happen. Bear in mind, however, that a criminal never checks your front door. They always check the back of your house for open windows. And the situation is no different online. You need to start thinking like a criminal. As a company you must ensure that you have made the necessary cybersecurity arrangements for strategic matters. It’s the only way to avoid a lot of misery. Find good hackers is the main challenge: do you do this yourself, through a platform, etc. Unfortunately, there is no uniform certification for hackers for now.”

Jonathan Bouman works as a GP but is also a hacker. During his medical studies he spent a lot of time programming and actively securing personal data. As a GP, he soon realised the importance of properly securing his patients’ digital medical and personal data. By working as a hacker and sharing his knowledge of cybersecurity, Jonathan makes a positive contribution to this.

Wietse Boonstra has spent several years working as a security researcher, bug bounty hunter and hacker. He discovered a vulnerability in Kaseya, which had a global impact. Wietse has been interested in cybersecurity from a young age. Initially a hardware hacker, he later started testing ‘everything he encountered on the internet for vulnerabilities’. He reports any (potential issues) to the owners, because it doesn’t benefit anyone if this information is out there on the street and companies go bankrupt as a result.”

Which responsibilities do you have as a hacker?

Jonathan: “If I find a leak, I know how far I can go. Usually you can combine several small vulnerabilities to find a larger vulnerability. As a hacker you are also always looking to strike the right balance. When is the error found relevant enough to report it and where should I look to clarify its impact. By informing companies about the next steps that I would take myself, they can ensure that the vulnerabilities that are found are properly and completely resolved.”

Wietse: “For me, as a hacker, I stop at stealing data that you gain access to because of a vulnerability. If you are able to create a dump of the database of a large insurance company, you simply pass this on to them and that's where the story ends. If a code enables you to get into a particular system, then you must choose the least harmful code to show the system’s owner that this vulnerability must be fixed. You never cripple a system altogether, by any means.”

What does a hacker need to do a good job?

Jonathan: “My tip for organisations that want to work with hackers is to build a relationship with them. Keep hackers informed about the vulnerabilities they reported. Involving hackers in what you do increases their motivation to continue contributing to the security of your business. Share resolved vulnerabilities so that others can learn from them and thus enable them to search (even) more effectively for gaps that need to be closed. Dare to share knowledge - that applies to hackers as well as companies. Keeping knowledge to yourself won't make the internet a safer place. Share knowledge as soon as possible and provide a safe environment in which hackers can do their job.”

Wietse: “Companies always stand to benefit when hackers monitor the the organisation’s security. So make sure that you lay down clear rules, whether or not in the form of a Coordinated Vulnerability Disclosure, on the basis of which you give hackers the opportunity to make a good contribution to this. I think it's important that the reward you get for a reported hack is commensurate with its value to the organisation. You don't just report a vulnerability, you make an organisation a bit more secure which is why it’s always nice that you get something in return that you can buy something for yourself. Hackers also need to make a living.”

CHAPTER 2
PREPARATION OF THE INTERNAL ORGANISATION

If a company or organisation wants to tackle its digital resilience, it needs to start by creating the conditions for effectively achieving this. Everyone must be aware of their own responsibilities and understand how they can contribute to increasing this resilience. They must have the required knowledge, capacity and resources for this. Another point for attention is the mutual collaboration between departments. The only way to counter unwanted digital attacks and prevent data leaks is by working together. Modern and adequately deployed ICT systems and infrastructure are another prerequisite for cybersecurity; as are well-secured ICT and vulnerability management processes. A close collaboration with a hacker community whose values overlap with your organisation's is the cherry of the cake of the continuous monitoring and improvement of your cybersecurity. This chapter discusses these subjects in more detail.

> *Cybersecurity is not something you do alone,*
> *it is a joint responsibility*

2.1 INTERNAL DEPARTMENTS

All the departments of an organisation play an important part in cybersecurity. In a municipality, each department or service must ensure that it consciously deals with (the protection of) sensitive information. And secure websites, systems and applications in such a way that the chances of misuse are minimal. Two disciplines in particular are important for the operational side of your organisation's cybersecurity: security and ITC. A good collaboration between the two ensures that technical risks are detected in a timely manner, are translated into a potential risk in the appropriate manner and, where necessary, are resolved in an adequate manner, within an appropriate time frame.

Security organisation

We have already mentioned this several times in this e-guide: cybersecurity and information security are becoming increasingly important. On the one hand, because of the desire to use products and services any time and anywhere, resulting in an ever-increasing demand for digital services. On the other hand, as a result of our growing reliance on digital information. (New) laws and regulations largely determine how the government and companies must guarantee the security of their systems and information.

Security department:
Basic requirements for proper operation

- Described roles and responsibilities (who does what in the context of cybersecurity).
- Clear policy that is embedded in the organisation at a strategic, tactical and operational level.
- Active monitoring of compliance with the agreements.
- Willingness to work together to ensure optimal protection

The security organisation, which is headed by the Chief Information Security Officer (CISO), must deploy an efficient set of measures, designed to guarantee the confidentiality, integrity and availability of information within a company or government institution. A cybersecurity and information security policy is only deemed successful when measures and regulations are embedded in the organisation at strategic, tactical and operational level. This means that everyone in the organisation knows what is expected of him/her and that the conditions to do the right things have been met. In addition, compliance with the agreements must be checked, whereby people are actively approached about possible points for improvement. Open, transparent communication ensures people are continuously engaged and informed. Especially (but not exclusively!) in the event of an emergency.

The security organisation, specifically the Information Security Officer (ISO), ensures that the potential (technical) risks are translated into risks for the organisation. This is done after determining in consultation with ICT which data and systems are threatened, in addition to the probability and impact of these threats. In the case of a municipality, the ISO is so well aware of the interests of the service for which he works that he can situated the detected (technical) risk in the right context and knows which systems and parts of the infrastructure may be at risk. Based on this information, the ISO can inform the director of the service about the possible implications of the identified risk and advise which measures should be taken. As such, the ISO ensures that the director can make a well-founded decision about the actions to be taken.

Cybersecurity is not something that is maintained on weekdays from 9 to 5. It requires continuous involvement, solid processes and a solid foundation.

To do its job adequately, the security department depends on the available knowledge, experience and necessary tools/resources at its disposal. In addition, the quality of the information the department receives is a determining factor. What is the exact vulnerability, in which system was it found, what are the technical implications, and which services use these systems? To operate properly, the security department needs back-up from management and must have a sufficient mandate to act quickly and properly in the event of calamities.

Security involves so much more than frameworks, policy and control. Insight into the implications of technical risks, knowledge of a department's or service's processes, good and timely communication, and mutual trust are just as important for guaranteeing adequate (digital) security.

ICT organisation

In order to provide the security department with sufficient and high-quality information about possible security risks, the ICT department must have a very wide range of (often specialist) knowledge, experience and supporting tools. ICT must also never never lose sight of the fact that cybersecurity is not an 'IT matter', but the concern of the entire organisation.

In addition, cybersecurity is not a temporary project, but a permanent daily task. ICT provides support for the implementation of the security policy, ensuring the organisation's continuity. Various tools can help you to continuously test your attack surface, which risks you run and which options are available to you to mitigate them. People, processes and technology are the three elements that determine whether your ICT department is sufficiently prepared. The extent to which you can use these elements is determined on the basis of the resources you can make available for this versus the degree of risk appetite.

An organisation rarely has all the necessary expertise in the field of cybersecurity available in-house. In terms of the **'people'** aspect, you can start by asking yourself whether you have the necessary specialists in-house, or whether you need to temporarily hire them from third parties. Usually the solution is a mix of both, with a ratio that is different for every organisation. The Municipality of The Hague receives support from various parties with specialist knowledge in the fields of technology and cybersecurity. During the selection, we take into account the quality of the solutions or services provided, as well as the willingness to walk through the various stages of the cybersecurity journey with us. Working as equal partners with third parties based on complementary knowledge and expertise determines how much of a difference we can make in terms of the resilience of the Municipality of The Hague. Where possible, we ensure that the people involved have the mandate they need to implement change - whether solicited or unsolicited.

In the context of the correct deployment of people, we also always highlight the form and content of communication. In addition to reporting a technical vulnerability, your ICT department must also explain the risk this involves for a specific department or system. The probability of the risk is also a determining factor for the measures to be taken. Communication by ICT stands or falls with the extent to which it is adapted to the knowledge of the target group for which it is intended and the channel that is used to convey the message. Involve everyone in what you do: both ICT and people within the organisation. Remember, the latter will have to resolve the vulnerabilities. The faster they take steps, the less they will have to resolve. That is why we invest so much time and effort at the Municipality of The Hague in informing all the parties concerned. By providing an insight into the positive effects of people's efforts, we ultimately expect to get everyone to the point where they start thinking along and tackle risks before they become problems.

An effective IT department has **clear processes** , paying attention to matters such as asset management, patch management, change management and vulnerability management. These are discussed in chapter 2.2.

As soon as the 'people' and 'processes' elements have been properly defined, you can, as indicated earlier, look at which **technologies** best meet this need. We discuss the following in more detail in the 'supporting technology' section in Chapter 2.3:

- software that helps to provide an insight into your organisation's digital footprint and attack surface,
- systems that help to coordinate and provide an insight into various activities and
- bug bounty platforms that allow you to shape your collaboration with hackers.

Teamwork

The people in the security expertise centre of the Municipality of The Hague work together closely, based on mutual trust. Peter van Eijk, Information Security Manager at the Municipality of The Hague: "There is plenty of conflict within the team, but it always relates to the content. You do not always have to agree with each other. The most balanced advice and the best results are achieved after robust discussions. Ultimately there can be no shine without friction. At the same time, there is no point in going crazy, either. This mutual cooperation is based on trust. We deliver in accordance with the agreements made and give advice based on solid arguments with which the business can assess which actions are necessary.

Questions to determine whether your IT department is ready for structural improvements in the field of cybersecurity

- For which percentage of assets is the responsible party unknown?
- Do I have an insight into the attack surface of our organisation at all times?
- Do we see cyberattacks coming?
- How often do we test the data security of our systems?
- Are we able to adequately prioritise and monitor the results of these tests?

> People, processes and technology determine whether your ICT department is sufficiently prepared.

Representatives of the security and ICT departments of the Municipality of The Hague are available 24/7. A specialist is always on hand to help if necessary. When our CISO calls because he has seen a new development or threat in the outside world, we usually are already working on it. By properly organising the front end of the process, we are able to identify potential threats in good time, scale properly, and take the appropriate measures to prevent the situation from getting out of hand. Employees and managers of these departments often find that work blends in seamlessly with their private lives because they take a personal interest in this field. They use every spare minute to keep abreast of the latest developments through online forums, events, webinars and other sources of information. There is more to digital security than technology. This too is and will always be the work of people.

The security expertise centre serves both the IT department and the rest of the organisation. In this way we increase the impact on the activities carried out within the city, we give clear direction to activities and we channel communication and activities in an adequate manner. Sparring together is also easier this way. These days, a cyberattack on the Municipality of The Hague is much more than a safety and ICT issue. It involves an attack on the entire, municipal Security Expertise Team, ICT and the business.”

> The trick is to start small and work your way up to the dot on the horizon, inching closer step by step. Determining for each use case what is needed to achieve this and how this can be arranged will eventually lead to an organisation that can professionally deal with hacks.

2.2 SETTING UP PROCESSES

There is a continuous interaction between the processes and tools that are used in the context of digital resilience. The tools give us insights on the basis of which we optimise our processes. For example, if we see that certain vulnerabilities occur in different places, we can also deploy successful solutions in other places. If specific defects recur repeatedly, we simply adjust our connection conditions accordingly. Every time we take another step, further refining our processes, new requirements and wishes automatically emerge for our tools. When setting up processes, you always have to start somewhere. A number of important processes are described below, which you can use to lay the foundation for the implementation of your cybersecurity policy and strategy.

Asset management

With ICT asset management you manage the inventory and life cycle of your organisation’s ICT resources. Hardware, software and associated licenses must be continuously maintained, updated, repaired and replaced. Good asset management provides insights into the ICT resources that an organisation possesses and the process that is needed to keep this data up to date. If this process is properly organised, you will have an insight into all your organisation’s assets and will know under whose responsibility they fall. Both are necessary for the continuous implementation of improvements in the context of cybersecurity. Asset management can be done by your own organisation or be outsourced to a third party.

Patch management

The next process that plays a vital role in cybersecurity is patching. A patch is an installation file that fixes a vulnerability or error in a programme or improves a programme by, for example, adding functionality. Vulnerabilities in a programme or website pose a potential threat to an organisation's information security. That is why every company should have a good plan of action to resolve detected vulnerabilities as quickly as possible. Patching is often a complex process because one change can affect multiple systems. The trick is to fix errors in the desired place, without (unintentionally) creating new problems in other places. Patches are therefore extensively tested before they are implemented. This can be done manually or automatically. You can only successfully implement the cybersecurity policy you developed with a tightly organised patch management process that allows you to implement patches 24 hours a day, 7 days a week.

Change management

The third process that plays an important role in cybersecurity is the process of implementing change. Change management is defined as the methods and ways in which organisations implement changes in internal and external processes. This involves preparing employees and offering them support, determining the necessary steps for implementing the change, and checking activities before and after implementation to ensure that the change has been correctly implemented. Large and small changes to ICT systems can cause problems because they have an impact on all kinds of parts, systems and people within an organisation. Good communication about the changes to be made is therefore one of the most important success factors of effective change management. Ensuring that you have a solid foundation to build on in your ICT department also means that having a structured approach for implementing changes.

At the Municipality of The Hague, any adjustments of ICT components are structurally implemented through the change management chain to ensure that we do not overlook any elements that may be impacted by this change. In most cases, necessary changes are implemented across departments and services. A careful, controlled and secure way of implementing changes therefore largely consists of intensive consultation with the parties involved. Which interventions are needed, what is the risk of these actions, how long will the relevant systems be unavailable for the service? The turnaround time of the adjustment and the type of service that is affected determine when is a good time to implement an action.

For example, we will not patch the cash register system of the city's swimming pools on a sunny day when half of the city is queueing outside to get in.

Vulnerability management

The fourth process concerns vulnerability management. This includes all the activities that an organisation undertakes to continuously ensure that vulnerabilities in its own digital systems are identified and repaired. A process in which potential vulnerabilities of digital assets are proactively identified, analysed, scaled and resolved. The entire life cycle of the vulnerabilities is monitored from A to Z to avoid any potential risks. No matter how complex the environment is. Vulnerability management is about risk acceptance and mitigation. If the security and IT department come to the conclusion that there is a vulnerability with a negative impact on the organisation, they can take measures to minimise the risk. But the owner of the affected systems is ultimately responsible and determines how to deal with the risk and the advice.

Despite recent reports of major hacks and costly consequences, many organisations still tend to take minimal measures when it comes to cybersecurity. Standard patch management and antivirus software are insufficient in terms of defence. They don't deter the average criminal. By continuously performing vulnerability scans, you keep informed about the changing threat landscape and vulnerabilities that may go unnoticed in daily practice are revealed. Developments and trends emerge from the accumulated history that determine whether the cybersecurity measures that you implemented are still effective in the field of people, process and technology.

TIPS

- Use the standard change management processes for security-related changes. This ensures that those involved will be more inclined to adopt these processes. The turnaround time of security adjustments is the only thing that deviates from the standard.
- Make clear agreements with your support department, provide guidance and information so that they can properly asses whether something is a security incident or not. An employee who receives a phishing e-mail is not a security incident; it becomes an incident, however, the second the link is clicked.
- Warm transfers to the IT department are preferable for security-related changes with high priority. This clarifies the need for speed much earlier in the process and also increases the chance that the IT team will devote their time and attention to solving the security incident as quickly as possible, setting aside their usual work.
- When in doubt, always have the IT team liaise directly with their colleagues in the security department.

If you go one step further, you can have penetration tests (pentests) performed. This involves deploying specialised hackers who use the vulnerabilities they find to break into systems and see how far they can get. These tests provide interesting insights into how difficult or easy it is for specialists to break into your systems and how easily sensitive data will be exposed. In the next chapter, we will discuss various forms of technological support that contribute to improving your organisation's cybersecurity.

Security and ICT classify a vulnerability as negative and impactful and recommend measures to minimise the risk. Ultimately, however, the owner of the affected systems is responsible and determines what happens to the risk and the advice.

2.3 SUPPORTING TECHNOLOGY

Technology plays an increasingly important role in our daily lives, including in robust cybersecurity. What does this support consist of? Applications that provide an insight into which information, websites and systems you have at your disposal and who ultimately is responsible for this. Systems in which you can record relevant data and track developments so that you can use the available time, money and capacity as efficiently as possible. And finally, platforms to work with hackers and to use their knowledge and skills to discover vulnerabilities before criminals misuse them.

Think big, but start small. Don't immediately turn on all the available options. Start with a limited scope: how are the internal processes organised, are all your assets registered? See what works and what doesn't and slowly expand it.

By focusing on strategic partnerships with the relevant suppliers when choosing supporting technology, you will increase your knowledge and experience, which in turn enables you to raise awareness of cybersecurity and resilience within your organisation.

Digital footprint and attack surface

When the Municipality of The Hague decided to step up its cybersecurity efforts in 2007, the organisation's digital footprint and attack surface were relatively undefined. A digital footprint refers to all the traces that a person leaves behind while using the internet. Information sent online, such as, for example, completed forms, sent emails and attachments, uploading videos or digital images and any other form of transmission of information. Traces of personal information that reveal who you are and what you do thus become available online to others.

An organisation's attack surface consists of various assets such as websites, domains, servers and host services that can be attacked in various ways, allowing the intruder to intercept data. By analysing and controlling your organisation's attack surface, you can reduce the risk of cyberthreats. Something that both large and small organisations should be actively doing. Because if you have no idea which systems and websites your organisation has, you cannot adequately protect them and you have no concept of the ramifications of an attack.

Analysing and managing your organisation's digital footprint and attack surface can be done in-house or outsourced to a specialist. Using platforms that were specially developed for this purpose, the assets of your organisation are listed and monitored. At the Municipality of The Hague, we have chosen to use Cybersprint's Attack Surface Management platform for this. Key elements that influenced our choice include the platform's broad usability and scalability and the agreements we could make with the supplier about the service levels we wanted.

Criteria for selecting an ASM platform

- Automation (scalability)
- Integration in processes
- Custom reporting

On average, 30-35% more assets are unearthed through these types of platforms, which is significantly more than what organisations usually have on their radar beforehand. And each asset has its own vulnerabilities. Mapping out the playing field and the associated risks is one thing, but a proper follow-up is an altogether different manner. That is why it is crucial that your internal processes are aligned with this and that you have the manpower to follow up on this within the organisation. One of the things we soon realised is that it is very difficult to identify the owner of the assets, i.e., who is responsible for solving the vulnerabilities found. And once the owner has been identified, convincing these people to take action or creating a sense of internal urgency to push through an upgrade can be challenging.

Because we are increasingly transferring software into the cloud at the Municipality of The Hague, we find it important to know which security risks we run in our supply chain and understand which vulnerabilities are at play. The Cybersprint platform helps us quickly gain an insight into this, after which we effectively engage in a dialogue with third parties about their security measures. The platform also forms an important link in the detection of shadow IT and malicious websites.

In addition to the vulnerabilities that you identify through your own efforts, there are numerous organisations that have information about hacks that are known worldwide. Organisations such as the IBD, NCSC and hacker websites continuously monitor what is going on and give advice on how to deal with findings. Experience has shown, however, that you should not solely rely on the recommendations of third parties. You must always think very carefully about the specific consequences for your own organisation. Other measures may have already been taken, sufficiently mitigating the risk as a result.

The latter helps us to identify possible phishing attacks at an early stage and to take measures to mitigate this risk.

At the Municipality of The Hague, we have consciously chosen to map our digital footprint and establish an inventory of it, in addition to monitoring our attack surface in a phased manner. We have thus been deploying more and more modules and expanding our services step by step. Starting with the Attack Surface Management platform, followed by the Social Media module and the Management module. The next step is to deploy the DMARC Monitor to better secure our e-mail flows and to deploy the platform even better to more easily meet the requirements set in the Baseline Information Security Government (BIO). The tools we work with actually help us to achieve the objective of 'preventing the exploitation of technical vulnerabilities'.

Purchasing tools to monitor your digital footprint and attack surface is a first step. Successfully following the recommendations for reducing risks ultimately determines the added value that you create for the organisation. Applications that help to schedule and track the necessary activities significantly contribute to this, because they are efficient and help to keep an overview. The main coordinating systems are discussed below.

> A good tool is first step. Successfully following the recommendations to reduce risks ultimately determines the added value for the organisation.

Coordinating systems

The adequate follow-up of identified vulnerabilities is a matter of making choices and where possible using supporting technology. Both are equally important. With regard to making choices, the following applies. You can scan the whole world with the technology that is currently available. Unfortunately, this yields so much information that you won't know where to start and what to do. Limit your scope, start by focussing on what is needed to properly protect your organisation's crown jewels. Focus on things that can really hurt you and problems that are easily solved. Keep in mind that it is impossible to solve everything at once. As long as you are familiar with the risks and can make a well-considered decision on whether you should tackle something now or later, you are in control. The second point, using supporting technology, concerns the increased

Considerations when evaluating coordinating tools

- Can backlog be included?
- Can we simply assign use stories to the right disciplinary team?
- Single or multiple use of data?
- What are minimum requirements for reporting?

automation of activities to be performed, human actions. If you work according to a fixed process, such as the 'Plan, Do, Check and Act cycle', you minimise the chance of making mistakes and prevent crucial steps from being overlooked.

Coordinating systems help to reduce administrative overhead. Reporting is vital in this context, preferably in the form of dashboards so that the organisation's management is based on well-substantiated arguments. The Municipality of The Hague believes in a more data-driven and information-driven approach, which is why we have selected various tools. We don't perform a one-off evaluation and selection. Instead, we constantly test whether systems still contribute to the set goals or whether we are bogged down in an administrative exercise.

> Agile working always conflicts with processes. Agile is about self-organising, about initiative. But to what extent is an ISO or an IT employee allowed to implement changes without the impact of said changes being investigated by others? The right coordinating tools help to coordinate actions across departments.

Configuration Management Database (CMDB)
You want to integrate the assets that you have uncovered by mapping your organisation's attack surface in a database in a structured way, together with the associated risk classification. This data can be recorded in a Configuration Management Database. Structural registration ensures that the information remains up-to-date and that the various assets are effectively managed. Because the amount of assets and (potential) vulnerabilities found is often greater than the available capacity to solve them, you can choose to temporarily 'park' any assets that you are not responsible for. When dealing with these assets, you must follow the prioritisation and action perspective (what are possible solutions for the issues that were found) that are suggested to you by the platform that monitors your attack surface and digital footprint. You must prioritise vulnerabilities in systems that have a direct impact on the continuity of your services in the event of a failure.

At the Municipality of The Hague, we have also included low-hanging fruit in our approach: issues that are easy to resolve that show that investing in cybersecurity is worth our while, preventing many problems.

ICT Service Management Systeem (ITSM)

ICT Service Management stands for the process-based management of the activities associated with the ICT management of an organisation. The ICT Service Management System is based on ITIL processes, which stands for Information Technology Infrastructure Library. This library describes the best practice solutions in the field of Information Communication Technology management. In other words: guidelines that indicate how an ICT service provider or department can guarantee that its customers receive the products and services they require. Adjustments to the ICT infrastructure are implemented in a structured and coordinated manner using an ITMS and the aforementioned ITIL processes. An extensive impact analysis is performed in advance and good backups are provided ensuring you can go back in time to the instant before a problem arose or before a change was implemented.

Are you certain that backups are correctly performed within your organisation? Every now and then, restore the complete backup of systems and check whether this leaves something to be desired in terms of consistency and completeness.

ITSM helps IT departments manage and control these processes. The ITMS can be used for:

- Configuration management/ICT asset management with which all relevant information about your configurations and the individual ICT resources is documented and maintained.
- Incident management, one of the most important duties of your ICT department, because this ensures that you can respond to incidents quickly and in a customer-friendly way.
- Problem management where common incidents are identified using the software and necessary follow-up steps are taken to prevent similar incidents in the future.
- Change management with which you keep track of which changes and adjustments you make in your IT environment.

Coordinating applications are available in the market as standard products. Which one is best suited to your organisation depends on the mission that you have set yourself, the requirements that the functionality must meet, and its integration with existing solutions within your organisation. The proper organisation of internal processes determines the contribution that systems make. So start by thinking about who within the organisation is responsible for addressing, assessing and pursuing reported vulnerabilities.

In the ICT Service Management System of the Municipality of The Hague, desired actions for resolving vulnerabilities are now automatically converted into work sheets for employees who set to work with them. They are signed off in the same system, after which a check is performed to see whether the follow-up was effective. We use the resulting new insights to further optimise existing processes.

Bug bounty platforms

More and more organisations and software developers are launching their own bug bounty programme in order to use the knowledge of hackers to detect vulnerabilities in online applications and websites. Before introducing a bug bounty programme, add a Coordinated Vulnerability Disclosure to your website to indicate that your organisation gives hackers the opportunity to share found vulnerabilities, without this having legal or criminal consequences. The Coordinated Vulnerability Disclosure and bug bounty programmes are discussed in more detail in Chapter 2.4 (Involving a hacker community).

BUG BOUNTY PLATFORM IN ACTION

Zerocopter supplies the platform that the Municipality of The Hague uses for the execution of its bug bounty programme, which is also used to register hacks that were detected during Hâck The Hague. Chantal Stekelenburg, Head of Operations, and Edwin van Andel, CEO of Zerocopter, explain how this type of platforms can make a difference.

Edwin: “We use the Zerocopter platform daily to facilitate communication with hackers who work for us at clients. They can find the client's briefing on the platform before getting started. The platform is also used for bug bounty administration, meaning to record hacks and determine what compensation hackers are eligible for. We also use the platform to make available templates for Coordinated Vulnerability Disclosures to companies”.

“During Hâck The Hague, the platform is also used to register vulnerabilities that were detected”, Chantal adds. “My place is ‘at the other end of the system', together with representatives of the Municipality of The Hague, to review all the incoming hacks. Is this a real vulnerability or is it a duplicate? How great is the impact? Is the report on the hack complete and clear? We then determine which hacks we think qualify for a prize and why. Ultimately, the jury decides who the real winners are. An additional advantage of the platform is that a time code is added to the logged hacks. This comes in handy in case identical hacks are logged in quick succession. This allows you to see who identified it first, down to the second.”

Edwin: “These bug bounty platforms are continuously developing. New functionality is added that makes life easier for hackers, for example by expanding the categories that hackers can choose from to find a suitable label for the vulnerability they have found. Other functionality focuses on the organisational side of the bug bounty programme, such as the common vulnerability scoring system calculator that helps determine the impact of a hack found using certain formulas. For example, if a lot of steps are required before you arrive at the vulnerability found, the chance that this will actually happen is smaller and the impact is therefore lower. If a user needs to interact with the system for a hack to succeed (for example, by clicking on a link) the likelihood that the hack will ever occur decreases. The new calculator takes all these elements into account.

But the hackers who work with the bug bounty platform make the greatest difference. By deploying a bug bounty platform, your organisation gains access to the knowledge and skills of vetted experts from all over the world. After defining a specific project, you receive well-written and validated reports to your own dashboard.”

We chose to work with the Zerocopter platform for the proper management of the Municipality of The Hague's bug bounty programme. Hackers report found vulnerabilities through the platform. The supplier's willingness to make a proactive contribution to the Municipality of The Hague's digital resilience in addition to the platform's functionality of the platform cinched the deal. Zerocopter also maintains good relations with a large hacker community, a crucial factor for the programme's success. Other benefits are that any hackers who use the platform are pre-screened and alleged vulnerabilities are properly reported.

We also communicate with hackers through the platform, rather than by e-mail. This prevents third parties from intercepting and misusing identified vulnerabilities. The Zerocopter experts also perform an initial triage of the reported vulnerabilities on our behalf. This allows us to optimally deploy our own employees when it comes to interpreting the possible impact on the availability of our systems and coordinate with the affected services. Zerocopter also handles the financial aspect of the programme. They can do this much faster with less effort than us, increasing cost efficiency as result.

2.4 INVOLVING A HACKER COMMUNITY

ICT is developing at lightning speed and the same applies to the tools and techniques that criminals use to break into systems and misuse them to their own advantage. The rapid pace at which changes take place and innovations see the light makes it almost impossible to make optimal use of the possibilities offered by technology without the assistance of external specialists. When it comes to cybersecurity, hackers are the experts. Ethical (honest) hackers are people who search for vulnerabilities in software and hardware, such as websites, computer systems and networks. Instead of disclosing these vulnerabilities, they inform the relevant organisations about the vulnerability to give them the opportunity to resolve this issue.

Despite the fact that hackers are still viewed with suspicion by many organisations, they have already prevented many a disaster. They help companies and government institutions to identify security risks and improve cybersecurity in a targeted manner. If you decide to work with hackers, make sure you take this community seriously. If a hacker detect a vulnerability in your systems himself or on request, respond quickly and communicate transparently. Keep the reporter informed of any progress made until the vulnerability is resolved. In terms of reward, steer clear of cool T-shirts and mugs. Make sure that the reward and credits a hacker gets for reporting a vulnerability are commensurate with the problems that his discovery has prevented.

To build a good relationship with the hacker community, you must work with suppliers and partners who are well-known in the hacker community and who have a good network within this target group. Find out below how to professionalise your collaboration with hackers step by step.

Coordinated Vulnerability Disclosure (CVD)

The purpose of a Coordinated Vulnerability Disclosure (formerly Responsible Disclosure) is to improve the security of ICT systems by sharing knowledge about vulnerabilities so that others can benefit from them. By including a CVD policy on the website, an organisation gives hackers the opportunity to share found vulnerabilities with this organisation, without negative consequences for the hacker. The CVD policy includes rules for both the hackers and the organisation itself. The hackers agree to a coordinated disclosure of a vulnerability after it has been fixed. The organisation will not sue the hacker for breaching its systems and will keep the reporter of the vulnerability informed of any progress that is made in resolving it. There are several informative websites that offer an initial CVD draft that you can customise as you see fit.

Bug bounty programme

By setting up a bug bounty programme you go one step further than the CVD. You pay a reward for every vulnerability that a hacker reports to you under the CVD. A bug bounty programme essentially is a reward programme for detecting vulnerabilities in an organisation’s IT systems and infrastructure. It's a nice addition to regular tests and checks of existing security measures because it attracts a larger number of people who will continue to test your systems over time. Does your organisation have a large amount of sensitive data and/or are the consequences of a criminal hack potentially large? Then using a bug bounty programme is definitely worth your while. These programmes give you the opportunity to take advantage of the skills and knowledge of a large network of hackers, enabling you to prevent data loss and reputation damage.

> Does your organisation have a large amount of sensitive data and/or are the consequences of a criminal hack potentially devastating? Then using a bug bounty programme is definitely worth your while.

At the Municipality of The Hague, we have chosen to let the hacker take the initiative and communicate on the vulnerability. Once the detected vulnerability has been resolved and released, the hacker may communicate about it so that others can benefit from this. Another conscious choice we have made concerns the moment of payment. In most cases, bug bounty programmes only pay out the reward based on proven results. This is an effective way to spend security budgets. Initially the Municipality of The Hague paid hackers when the hack was resolved. In some instances, they had to wait quite a long time for their cash. Now we pay the bounty as soon as we accept a vulnerability that has been found. This has had a very positive impact on the number and quality of vulnerabilities that are reported to us.

Tips

- The moment of payment influences the number and quality of the reported vulnerabilities.
- You can outsource the financial handling of reported hacks to the bug bounty platform you work with.

Hackathon

Many companies use hack events or hackathons to solve a specific problem, to develop an innovative business plan or to arrive at new insights within a short, set time frame. However, the hacking event that we discuss in this e-guide involves inviting hackers to look at which vulnerabilities they can find in the systems and websites of the organisation and suppliers that are part of the same ecosystem, at a specific time, while sticking to pre-defined rules. If such an event is well thought out, prepared and followed up, it can be a perfect addition to the organisation's existing cybersecurity programme. However, the organisation of such an effort also requires considerable efforts that should not be underestimated in addition to strict controls to prevent things from unintentionally getting out of hand.

Before your organisation decides to organise a hacking event, you must always check whether

- Your organisation is prepared, in terms of capacity, knowledge, processes and tools to properly register and follow up on the vulnerabilities they find.
- You have a good overview of your entire digital attack surface and you have already resolved or mapped any low-hanging fruit yourself.
- Good and watertight rules have been developed to ensure that the event runs smoothly.
- You, yourself or through partners, know which hackers to involve in the event and can approach them.

- You have the capacity to adequately develop internal and external communication around the event, both in terms of content and the channels to be used.
- The technical infrastructure is available to ensure the smooth running and monitoring of the event.

And finally, you want to make sure that you involve the right people in the event. Because although you may think that a hackathon is all about technology, ultimately it all boils down to relying on the right people. Enthusiastic, motivated, committed people who create an attractive, challenging, safe and personal environment where the knowledge and skills of others (the hackers) are maximised.

After making sure that the basic requirements were met, with the help of such partners as Cybersprint and Zerocopter, the Municipality of The Hague went one step further, organising Hâck The Hague together with Cybersprint. Initially our objective was to highlight our Responsible Disclosure (the precursor to Coordinated Vulnerability Disclosure). However, the event was such a success that we

GOOD TO KNOW FOR HACKATHONS

Which elements contribute to the success of an event such as Hâck The Hague? Chris van 't Hof is a presenter, researcher, writer and organiser in the IT sector. He has several publications to his name in which he describes the world of hackers and security specialists from the inside, and is thus best placed to answer this question.

Chris: “You may not expect this, but hackers throw the best parties. In order to also organise a successful hackathon, you must therefore have a very good idea of the culture you are dealing with. In my view, culture stands for 'a shared repertoire of habits and their symbolic expressions'. In the hacker community, the shared repertoire mainly consists of sifting through code and finding something that others have overlooked. Symbolic expressions in the hacker scene include the use of specific lingo, hoodies and colours when decorating the venue, to list just a few examples.

Another important factor that I would like to stress is that this e-guide is not a manual for organising hackathons, which for many companies equates a cheap (albeit often intensive) way to quickly develop innovative solutions or products. We are talking about hacking events where an organisation is serious about improving the online security of its systems.”

Hackers are people who make, break and discuss technology

As someone who regularly attends and organises hackathons and interacts with members of the hacker community, I believe that the following aspects influence the success or failure of a hacking event. The content is always more important than the form.

Content

- Purpose of the event - make sure it's really about improving the online security of systems and not about PR. Not “Look, we also work with hackers”. This is a big turn-off for hackers.
- The scope of the systems to be hacked – In other words, how much can really be hacked? Diversity and complexity combine to offer a sufficient challenge for hackers. An ex-

now organise it on an annual basis. We started out in 2017 with approximately 20 hackers, giving them free rein to hack a limited number of our own systems and websites. Four years later, we now welcome 200 professional and student hackers, who review a large number of municipal systems and websites to see whether they can be hacked. Every year, a growing number of the city's suppliers sign up, in hopes of taking the security of their own systems to the next level. Change is the one constant and that certainly applies to our annual hacking event. In 2021, we will be organising Hâck The Hague online for the first time ever, adding a completely new dimension.

In the next chapter we will go into more detail about the different aspects that play a role in the organisation of a hacking event. The aim is to allow you to hit the ground running with this information, ensuring you don't have to reinvent the wheel from scratch.

tra dimension is added when there are physical objects to be hacked that appeal to the imagination.

- Good follow-up - Will you do something with the vulnerabilities that were detected and inform the finders about actions taken? Some vulnerabilities can be fixed very quickly. Report this. But some things are more difficult to fix. You will then have to come up with good reasons why this is the case.
- Group Dynamics - Who else is coming? A hackathon is an excellent opportunity for hackers to meet others they only know from online or people with a relevant reputation.
- Jury quality - The people who ultimately evaluate your hacks have to be knowledgeable (credibility). If they are well-known, they will also attract many good participants.

Form

- Provide a pleasant, accessible location. Hackers just want to hack. They don't like a fuss. Location facilities are more important than status.
- Indispensable elements when catering a hackathon event are Club-Mate (a caffeinated and carbonated soft drink), snacks, Red Bull and pizza (but no alcohol!)
- Hackers love swag - the fashionable acronym for 'Stuff We All Get', or all kinds of promotional gifts such as hoodies, devices, stickers, keycords and the like.

Finally

Unfortunately, the hacker scene mainly consists of men. Cherish those few female hackers who want to join in, but don't overemphasise that they're there because it will make them feel uneasy. Also don't frantically invite women who don't know how to tack, to guarantee the gender balance, because this will achieve exactly the opposite.

Try to limit the number of journalists present or at least ensure that they do not bother the participating hackers too much. The same goes for bigwigs who are flown in for a photo opp with a hacker. Just don't. This will push all the wrong buttons.

All the above tips are not a guarantee for success. However, they can contribute to creating an authentic event that is in keeping with your organisation's mission and values."

CHAPTER 3
ORGANISING A HACKATHON

As with any other event, when organising a hackathon, the devil is in the details. Without attempting to be exhaustive, this chapter lists some key elements that form the basis of your hacking event. The following points are addressed:

3.1 Determining the scope and basic requirements

3.2 PR & communication points for attention

3.3 Preparation

3.4 Execution prior to event

3.5 During the event

3.6 Aftercare

Finally, Appendix 1 lists the key elements of the scenario for a hackathon.

3.1 DETERMINING THE SCOPE AND BASIC REQUIREMENTS

Determining the event's scope

- Date and duration of the event
- Determining a physical location or choosing an online environment (or both/hybrid event)
- Number of hackers and professional/student ratio and skills. When participants register, make sure you have a nice variety of hackers. Every hacker often has a certain method or specific knowledge of a tool. So focus on the skills and level of the hackers
- Make an inventory of which own systems and which supplier systems you will open up to the hackers

Basic requirements

- Inventory and reserve required capacity from various disciplines
  - Management backup
  - Project management
  - Communication & PR
  - Security
  - ICT
  - Partner management
  - Supplier management
- Determine required systems
- Develop and earmark required budget (direct/indirect)
- Develop frameworks
- Rules for participation
- Check potential legal implications
- Appoint jury members

3.2 POINTS FOR ATTENTION PR & COMMUNICATION

Points for attention PR

- Objective of PR activities
- Main and subthemes
- Parties/publications to be involved
- Communication channels to be used for PR purposes (own/third parties)
- Content to be created (articles, blogposts, videos, podcasts, etc.)

Points for attention Communication

- Target groups to be approached
  - Employees in own organisation
  - Partners
  - Hacker community
  - Suppliers
  - Citizens/public/clients
- Database of target groups to be approached
  - Which information do you need from each target group
  - Where will this information be saved
  - How can you ensure that this information stays up to date
- Required content by target group
- Communication channels to be used for each target group (own/third parties)

3.3 PREPARATION

Coordination team

- Set up project team
- Schedule and prepare brainstorming sessions
- Host brainstorming sessions and write out meeting minutes
- Draw up action plan and planning schedule
- Draw up budget

Project team

- Brainstorming event:
  Objective, target group, location, participants, stakeholders, internally involved, setup, medium, content of the contest, programme content, budget, prizes

Communication team

- Define objective and target group
- Develop brainstorming ideas for communication
- Assess what worked during previous events
- Determine and subdivide budget
- Draw up planning schedule
- Keep action list
- Prepare meetings
- Communication consultations

Technical team

- Draw up action plan and planning schedule
- Quotation Open VPN licenses
- Design dashboarding
- Design backend
- Inventory of low-hanging fruit
- Prepare scanning tools
- Weekly team meetings
- Visit venue
- Inventory of IT resources
- Presentation Management Team
  Execution & Management Hâck The Hague 2021
- Reserve capacity IT Basic Services
- Draw up planning schedule

3.4 EXECUTION PRIOR TO EVENT

Coordination team

- Keep an action list
- Set up meetings
    - Online platform
    - Approach parties to build platform
    - Request demo from all the parties involved
    - Request planning for the platform set-up
- Programme
    - Create draft programme
    - Finalise programme
    - Interviews with speakers
- Registration
    - Create form
    - Set up landing page for registration
    - Newsletter/Registration open e-mail
    - Updates to all the parties involved
    - Selection 1
    - Selection 2 (back-up)
    - E-mail selection confirmation of participation
    - Email non-participants waiting list/back-up list
    - Second round confirmation of participation backup list
- Video producer
    - Kick-off video
    - After movie
    - Videos for online program
    - Edit videos
    - Create transition images

Project team

- Draft day programme
    - Programme
    - Content - objective, target audience
    - Format
    - Execution
    - Select participants
    - Approach participants by e-mail
    - Record video (preliminary discussion, briefing, script, film, edit, check, finalise)
    - Record podcast (preliminary discussion, draft questions, interview)
    - Request and deliver speaker bio and photo for speaker page
    - Edit video and podcast: corporate identity, jingle, subtitles, translation
- Competition
    - Participants (number of countries and experience)
    - Prizes
    - Conditions
    - Rules
    - Jury composition
    - Brief jury
- Regular project consultations

Communication team

- Keep action list
- Prepare meetings
- Communication consultations
- Draft script
  - Target group hackers
  - Draw up and send newsletters
  - Create registration form
  - Order cup for winners
  - Mail information
  - Mail login details
- Target group student hackers
  - Draw up inventory of schools
  - Meetings with schools
  - Create information pack (online) Draft mail to schools
  - Approach schools
  - Register schools
  - Keep list of registrations
  - Selection of hackers
  - Contact the selected hackers
  - Request logos of schools
  - Draw up Q&A student hackers
  - Translate communication flow for hackers to student audience
  - Draw up letter of recommendation
  - Sign letter of recommendation
- Target group potential hackers
  - Contact platforms for the dissemination of HTH registration
  - Social posts
  - Through own networks of persons involved in the organisation
- Target group suppliers
  - Request testimonials from suppliers
  - Draw up e-mail to suppliers (2x)
  - Check e-mail to suppliers
  - Send e-mail to suppliers (2x)
  - Schedule day of calls to convince suppliers
  - Monitor supplier mailbox
  - Send follow-up message to suppliers
  - Upload logos and specs for each supplier
  - Coordination contacts with suppliers through one mailbox
  - Mail programme link + tweet proposal the day before the event
- Target group: the public, mainly through PR
  - Write, review and request green light for press releases
  - Send save the date
  - Send press invitation HTH21
  - Send reminder press invitation
  - Send press login/account information
  - Send press release after event
  - Monitoring
  - Write out media pitches
  - Guerrilla marketing

- Target group: Internal organisation
  - Announce HTH
  - Plan internal organisation
  - Mail programme link + tweet proposal the day before the event
- Podcast
  - Approach suitable people for an interview
  - Develop questions, interviews (online)
  - Edit podcast
- Video
  - Write scripts
  - Request quotes for subtitling
- Logistics & catering
  - Inventory of venues and booking
  - Order catering
  - Props to be used during the event (event decoration)
  - Set date and time for spokespeople
  - Check who needs a day pass
- Editor
  - Create banners
  - Design event decoration
  - Create map of countries wishing to participate
  - Design prize check

Technical team

- Implementation VPN solution
- Configure VPN solution
- Test VPN solution
- Technical solution backend
- Test backend
- Resolve low-hanging fruit
- Deliver dashboarding
- Test dashboarding
- Coordinate with Control Room
- Set up Discord channels

3.5 DURING THE EVENT

Coordination team

- Oversee programme
- POC video team

Project team

- General questions
- Available for the jury

Communication team

- Available for internal requests
- Available for media requests
- Moderator Discord

Technical team

- Stand-by for technical questions
- Organising technological set-up during the event
- Control room
- Moderator Discord

Logistics & catering

- Oversee catering
- Order pizzas
- Make sure that venues are available
- Oversee live interviews

3.6 AFTERCARE

Coordination team

- Send goodie bags
- Organise evaluation by the project team
- Send thank you to jury

Project team

- Evaluation project team event and results

Communication team

- Evaluation event and results
- Gather media coverage
- Request reviews from suppliers and participants
- Draw up e-mail to participants after the event (thank you/form/delivery time/survey)

Technical team

- Solution tests results
- Solution scan results
- Other remaining issues

Logistics & catering

- Evaluation of resources

ACKNOWLEDGEMENTS

The success of previous editions of Hâck the Hague is entirely the merit of a large group of people. Starting of course with the participating hackers as well as the motivated, enthusiastic core team of employees of the organisers: the Municipality of The Hague and Cybersprint. Below you will find an incomplete list of people who we wish to thank for their contribution to the organisation and fine-tuning of Hâck The Hague: Asmara Kramer (PPMO city-wide ICT Portfolio - Municipality of The Hague), Chantal Stekelenburg (Head of Operations - Zerocopter), Chris van 't Hof (Presenter, Researcher, Author and Organiser in ITC), Floor Terra (Senior Privacy Advisor), Letizia Luijs (Communication & PR), Liset Metz (Consultant Marketing & Communication - Cybersprint), Marieta van den Heuvel (Communication consultant Information & Automatation - Municipality of The Hague), Michel Slootweg (Information Security Officer - Municipality of The Hague), Peter van Eijk (Information Security Manager - Municipality of The Hague), Wouter Wouda (Graphic designer - Cybersprint).

ANNEXE 1 KEY ELEMENTS OF THE SCENARIO FOR A HACKATHON

Contents

CONTACT DETAILS

Project team

NAME & TITLE	E-MAIL & PHONE NUMBER
Budget management	
CISO	
Communication	
Coordination & Press	
President of the Day	
Facility	
Management support	
Marketing	
Technology	

Participants live day programme

NAME	PHONE NUMBER

Jury members

NAME + ORGANISATION	PHONE NUMBER

Facilities and AV media

NAME	PHONE NUMBER

Discord moderators

NAME ISO	USE OF THE ZEROCOPTER	USE OF SOCIALS
		A
	M	
		M

M = Morning
In the morning 10 am - 1 pm. Perhaps also coordinate in the afternoon.

Day = Whole day
Available throughout the day to provide assistance and support.

A = Afternoon
In the afternoon 1 pm - 4 pm. Perhaps also necessary in the morning Coordinate.

VENUE

Address

- NAW
- phone number
- contact person
- itinerary

Spaces

- Name and use of the space
- …
- …

AV resources

- Screens + HDMI cables
- Laptops and locations where necessary
- Support on the day of the event to ensure that screens remain operational

Roles of the people on-site

- …
- …

Catering

TIME:	TYPE:	VENUE:
08:00 - 18:00	Coffee and tea	
10:00	Muffins	
12:00	Lunch	
15:00	Cheese rolls	
17:30	Drinks	
18:00	Pizza	

PROGRAMME (CONCISE)

TIME	FORMAT	SEGMENT	SPOKESPEOPLE
09:30 - 10:00	Live	Timer that counts down to the start of HTH	
10:00	Live	... addresses hackers and crowd	
10:25	Video	Part 1/2 Kick-off	
10:27	Video	Part 2/2 introduction	
10:30	Live	... gives technical briefing to participants (live)	
10:59	Video	Transition screen	
etc.	etc.	etc.	

PROGRAMME + SCRIPT

Block 1: Kick-off

Time: **09:30-10:00 (30 minutes)**
Venue: -
Attending: -
Visual: Timer counting down

Time: **10:00-10:25 (25 minutes)**
Venue: Studio (foyer)
Attending: Chris, Jeroen, Pieter, Peter
Visual: Seated at a table. Opening event with …
etc.

Text <person>

- Welcome all to the first digital version of Hâck The Hague!
- We are live from the city’s town hall.
- […]
- Next to me is …..

Question from <person> to <person>

- A new year of Hâck the Hague. Are you looking forward to it?
- How did Hâck the Hague come so far?
- …..

[….To be developed in more detail for all the programme segments]

WHAT IF SCENARIOS

Internet drops

Issue:

Approach:

Solution:

Team:

YouTube live is hacked

Issue:

Approach:

Solution:

Team:

The screen of the broadcast goes black

Issue:

Approach:

Solution:

Team:

Hackers find very sensitive information

Issue:

Approach:

Solution:

Team:

VPN no longer works

Issue:

Approach:

Solution:

Team:

[…]

V1.0 // NOVEMBER 2021