mnemonic
SECURING YOUR BUSINESS

SECURITY 2019 REPORT

Security Report 2019

In the field of cybersecurity it can seem like every year surpasses the last. The volume and sophistication of attacks grow, as does the damage caused. As businesses and organisations become more dependent on technology, the impact of these attacks and the importance of securing technology increases.

As mnemonic enters its 19th year, we continue to evolve to meet the demands of today and position ourselves for the world of security one, two, five and ten years from now. In 2018, we took important steps towards securing this future.

First, we entered into a partnership with Ferd, an established long-term investment company. In an industry highly familiar with mergers and acquisitions, where innovative organisations are routinely absorbed by large vendors, this partnership ensures our continued independence, which is highly valued by our employees, partners and customers. More employees than ever are now shareholders in mnemonic, giving almost all of us a stake in the future of the company.

For our customers, this means we will continue our efforts to deliver quality and invest heavily into recruitment, training and R&D.

We also opened our first office outside of Scandinavia in 2018. This is one of several steps to increase our international presence to further support our growing global customer base. The next time you are in London, we welcome you to stop by our office in Canary Wharf.

mnemonic is growing steadily. We were joined by 40 new experts last year, prompting our upcoming move to bigger offices. We consider ourselves very privileged, as we manage to attract highly talented and motivated students as well as veterans, despite our industry's resource and skill shortage.

Now to this year's report: Our security experts, partners and customers have again written a publication that covers the spectrum of modern cybersecurity. For the seventh consecutive year, I am proud to present to you our Security Report.

Thank you!

TØNNES INGEBRIGTSEN
CEO, mnemonic

TABLE OF CONTENTS SECURITY REPORT 2019

ARTICLES

INTERVIEWS | STATISTICS

WORD ON THE STREET

2018 IN NUMBERS

ARTICLES


2019
SECURITY
PREDICTIONS

Jon Røgeberg
Head of Threat Intelligence,
mnemonic

I knew you would be here. Our psychic on retainer foretold this prophecy, and here you are. This prediction alone should be enough proof to convince you that our psychic – the revered Mystic Byte - is the real deal. Mystic Byte is only now recovering from their psychic journey into 2019 and beyond, where they traversed parallel continuums to unravel the singularity that represents our futures' true path.

The truths of 2019 and beyond have been validated by our crystal ball, cross-referenced with our tarot cards and plotted on our star chart. This is it.

When looking into what 2019 may bring us, there was no shortage of topics, trends and themes that rose to the surface. The rise of sextortion, the global impact of privacy regulations in the United States, hardware hacking, the continued gaping holes that exist in IoT, massive data leaks caused by cloud misconfigurations, the role automation has in incident response, so-called fileless malware and the increased use of legitimate tools for malicious purposes were just some of the topics considered for our 2019 predictions.

This year, under Mystic Byte's guidance, we have decided to take a more in-depth look at two topics: one that will have a high impact in the future, while the second has a high impact today already.

A QUANTUM LEAP TOWARDS TOMORROW'S SECURITY CHALLENGES

The lore of quantum computing has long been reserved for theoretical discussions amongst academics and the plotlines of sci-fi movies.

However, in the past five or so years, several tech giants, including Google, Microsoft, IBM, Intel, and Alibaba, have started heavily investing into quantum research. The Chinese government has pledged over $10 billion USD to build the world's largest quantum facility and the US and European Union are increasing their funding for quantum research. Make no doubt about it – the quantum race is on. ▸

The expectation is that quantum computing will become commercialised relatively quickly. IBM already announced their first commercially available quantum computer in early 2019, and cloud-based quantum services are already publicly available.

While the exact application and potential of quantum computing is still largely under debate, there are some fairly common beliefs about where it will be a game changer. Amongst these are accelerating certain computational tasks required for modelling and simulations (think medicinal research, discovering compounds and materials, space exploration and similar). Another use is the computational resources needed to solve very specific mathematical problems, such as calculating the prime factors of very large numbers.

One major milestone will be to achieve quantum supremacy. This is defined as when a quantum computer can reliably outperform a classical computer in solving a defined problem. How close are we to this milestone? Google is optimistic that Bristlecone, their latest quantum processor announced in early 2018, will prove quantum supremacy in the 'very near' future, and has partnered with NASA to validate the results.

So what does this have to do with security? Many modern encryption standards and their underlying cryptography utilise mathematics that rely on the prime factors of large integers. Factoring very large numbers into their prime "building blocks" is extremely difficult for classical computers, and this difficulty underlies the security of many cryptographic algorithms. While it is easy to factor the number 20 as the product of the primes 2 x 2 x 5, for example, factoring larger numbers becomes exponentially more difficult when using classical factoring algorithms.

In 1994, mathematician Peter Shor formulated an algorithm to factorise numbers on a quantum computer that would perform exponentially faster than the most efficient known classical factoring algorithm. "Shor's algorithm" was created decades before we had the quantum computer to test it on, and no one can imagine what researchers will invent when they have a reliable quantum computer to experiment with.

In short, this means quantum computing will effectively be able to break all cryptography and encryption standards that rely on prime factors or other calculations similarly susceptible to quantum processing. To put it into perspective, this includes the widely used RSA and ECC, which essentially threatens the entire public key infrastructure (PKI) we use for web security. There is also the billions of IoT devices that probably cannot be upgraded to support new standards, all that encrypted data that has been leaked in the past that is only being guarded by soon-to-be-broken encryption standards, and the list goes on.

NIST (the US National Institute of Standards and Technology) has started a competition to develop Post-Quantum Cryptography Standardization where players like Google, Microsoft, and a slew of others are actively pursuing the creation and adoption of encryption and cryptography standards – known as post-quantum encryption – that will be resilient towards quantum-enabled attacks.

History has shown that it takes a long time to migrate away from technology we have become reliant on. An example would be the migration from the hashing algorithm MD5 that was used in X.509 certificates, but was proven weak as early as in 2005. We already had other hashing algorithms that were stronger, such as SHA256, and migration should have been quick. It took Microsoft almost a decade to migrate its certificate authority (CA) off MD5. This was the means used in the 2012 Flame virus attack to fake Microsoft code-signing certificates. Microsoft finalised its migration off MD5 in 2014, a decade after it was well publicly accepted as an insecure hashing algorithm.

So when exactly should we expect these quantum-enabled attacks to become a reality? Well, no one really knows when quantum technology that can efficiently perform "attacks" will be commercially available (commercially available in this context excludes nation states who will likely have their hands on quantum technology long before it becomes commercially available in any practical sense). Despite this, 2025 has emerged as a target year for when our security standards need to be quantum-ready.

Now you may be thinking that this sounds like a problem for 2025 – and it is. But it's also a 2019 – 2024 problem as well.

The first challenge, which may not have a solution but certainly requires awareness, is that data that is leaked today, despite being encrypted, will theoretically be able to be decrypted in the 'near' future if it relies on any quantum-susceptible encryption standards. Although this data, and data leaked in the coming years can be perceived as "old" at the time that the encryption is broken, there are no shortage of industries and data types that are interesting no matter the age of the data. Think classified government documents, health data, personal data, passwords, patents, military secrets, and so on.

Some believe that nation states may already be recording encrypted web traffic and storing it until it can eventually be decrypted using quantum technology (NB: this in addition to encrypted traffic already being intercepted and decrypted using the DROWN and Logjam cryptography attacks). In October 2018, the state-owned China Telecom was accused of purposely manipulating BGP routes to hijack and re-direct traffic from the Internet's backbone through their own servers, before forwarding it to their intended destinations. Could this be a case of an honest misconfiguration at the hands of a network operator at China Telecom, or a nation state actively collecting encrypted information it intends to break using quantum technology (and now I pause to adjust my tinfoil hat).

The world is slow to adopt change when it comes to security. Even when we know our systems are vulnerable, we know there is a valid security patch to plug the hole, and we know there are active attacks exploiting this exact vulnerability, we are still nonchalant about installing security patches. Even after the global impact and media attention of WannaCry and NotPetya, there are hundreds of thousands of machines that remain vulnerable to EternalBlue, the primary infection route for these attacks.

Our prediction is that the moment quantum supremacy is proven and the inevitable media hype is in full swing, organisations will start to familiarise themselves with the issue. While it may not create Y2K hype, those who were working in security in 1999 will certainly have some eerily similar flashbacks.

Realistically though, history has shown (you can just look at the fiasco of organisations racing the deadline to comply to GDPR last May) that we will unfortunately need to be far too close to a definitive, determined deadline before organisations and society as a whole feel enough pressure to start taking the necessary collective actions to address this inevitable challenge. In this case though, similar to Flame and other incidents, the deadline will not be known until after it's too late.

DIGITAL EXTORTION GOES UNDERGROUND

2018 was a monumental year for ransomware. Not only because it retained its title as the key malware threat according to Europol's European Cybercrime Centre (EC3), but the term itself was added to the Oxford English Dictionary (along with *airplane mode, force quit,* and at the despair of content creators everywhere, the acronym *tl;dr* [too long; didn't read]).

Ransomware itself has evolved over the years. First dating back to 1989, being spread by floppy disks, ransomware's evolution has seen it take on many forms. From self-propagating worms, to systematically deleting users' data until a ransom is paid, and simply being used as a scapegoat to cover targeted attacks, the evolution of ransomware is only limited by the sinister imagination and creativity of cyber criminals. ▸

But, ransomware itself is merely a subset and evolution of criminal activity that dates back far earlier than the modern computer – extortion and blackmail. The premise of both is simple: pay up, or else. What exactly encompasses this "or else" threat varies, it can predominantly be divided into one of three categories that have remained largely unchanged even before the digital era: (1) *or else* I will reveal information that you do not want to be revealed, (2) *or else* I will destroy something of yours, (3) *or else* I will physically harm you or someone close to you.

If only criminals could find a way to curb these challenges: enter crypto miners

For those cybercriminals using ransomware as a money-making scheme, which is the large majority of cases, it is only effective if the victims actually pay the ransom. There are a variety of reasons for why a victim may, or may not pay a ransom. For example the victim may have a backup routine that allows them to simply rebuild their infected client and restore the data themselves, or the encrypted data being held hostage may simply not be valued high enough to justify paying the ransom. In other cases, a victim does not pay the ransom because they refuse to give in to the criminal's demands, or do not believe that the criminal will honour their part of the deal and decrypt the victim's data if they pay up. There are also cases where the criminal has made a technical error that does not allow a victim to pay, fails to encrypt the data as intended, or simply because the payment method – most commonly in the form of some cryptocurrency - is too complex for the victim. This last case has resulted in some criminals offering support services and step-by-step tutorials on how to pay with cryptocurrencies.

Exactly how many victims are paying ransoms, and in turn, how much criminals are earning from ransomware can only be estimated, and even then the estimates vary widely. The revenues are generally measured in the millions, while the damage caused is measured in billions. One truth that is known though, is that criminals will continue as long as it is financially beneficial for them to do so – meaning they are making a profit large enough to justify the risk, and there are no other money-making opportunities that are more attractive.

A challenge ransomware poses to criminals is that it relies on a victim's willingness to pay the ransom, and also requires the attacker to reveal that they have infected the victim's system. If only criminals could find a way to curb both of these challenges: enter crypto miners.

The concept of cryptocurrencies still baffle many people. For the purpose of this article, it is only important to know that cryptocurrencies require computational resources to calculate and verify transactions. Because cryptocurrencies are decentralised without a specific owner, the necessary computational resources to perform these calculations are provided by a vast network of people offering their own computing resources. As a reward for performing these calculations, there are occasional lotteries where crypto currency – coins – are awarded. The more calculations a person performs on behalf of the cryptocurrency, the more likely they are to be awarded a coin. The performance of these calculations for profit is known as crypto mining, and it is a legitimate business.

For cyber criminals, crypto mining is a seemingly perfect match that solves two of their major obstacles in maximising profits: the reliance on victims paying the ransom, and the requirement to reveal their infection to demand the ransom. Instead of infecting a client, encrypting data and demanding a ransom in exchange for the data, criminals simply install a crypto miner and do their best to remain undetected. Once the miner is installed, any malware (if any was used at all) can even be removed.

The likelihood of the victim noticing the crypto miner running on their client will depend on if they have the necessary security software to identify mining activity, or if they notice the side-effects of crypto mining – that is increased resources being used on clients and servers. This may be in the form of resource usage simply being higher than normal, a decrease in performance, or if at a large enough scale, an increase in energy consumption.

This is why from the tail end of 2017, and continuing throughout 2018, cybercriminals made a noticeable shift from the destructive, encrypting variants of ransomware to crypto miners. There is little doubt that criminals will continue to infect victims and enrol them into crypto mining activities throughout 2019. For how long criminals utilise this tactic will likely be reliant on society's acceptance of crypto-currencies, and thereby their value. Criminals will always follow the money, and perhaps our security regimes should do the same. For the time being, crypto mining can still be profitable, particularly for cybercriminals who hijack other users' resources. However, if the value of cryptocurrencies continues on their downwards trajectory, and the competition amongst miners continues to increase, we will reach a point where criminals find a more profitable or efficient method to earn money – that we can be sure of. ●

ARTICLE

Security Gatekeeping in a DevOps World

Mark Eldridge
Security Consultant,
mnemonic

AFTER READING THIS ARTICLE, YOU WILL:

- Understand how DevOps can let you react to vulnerabilities faster than a potential attacker
- Know when DevOps can be an appropriate approach, and when it is not
- See the importance of making the organisation outside the security department *security self-sufficient*

DevOps is rapidly gaining popularity and heading towards the mainstream. However, as with many frameworks and methodologies grabbing headlines, it is often without people understanding what it really is, or even more importantly, where it's appropriate to use. This especially has consequences when we are trying to adapt security to the era of DevOps.

Zane Lackey is one of the early pioneers of Secure DevOps. He describes his lessons learned while managing the security of the e-commerce website Etsy's transition to DevOps like this[1]:

During the early days of the shift away from Waterfall development, I was incredibly fortunate to be in the position of building the security team at Etsy while it was one of the first companies pioneering DevOps. At the time, for most companies, production application changes were typically made every 6 to 18 months. However, as I learned on my first day as head of security, Etsy was making production code deployments 20 times per day and rising. As you can imagine—and I had to learn the hard way—most of the classic approaches to security simply weren't going to survive in this environment.

So what exactly is DevOps? Well the definition can be quite rubbery. As Lackey put it, *ask 10 people, get 11 answers*. In general use, it tends to mean two things:

1. Rapid deployments of new software builds to production, sometimes dozens of times each day, and

2. Developers having direct access to production infrastructure.

This first component is related to the Agile software development methodology which sprang up in the early 2000s. Now however, the word 'agile' has become quite diluted, but in the context of software development it was popularised by the proclamation *the Agile Manifesto*[2] back in 2001. The Manifesto articulated key values and principles that its authors believed software developers should use to guide their work, and was itself a reaction to the methodologies in common use at the time: primarily the waterfall model. ▸

[1,2] *See Reference List at the end of the report*

The waterfall model had been copy-pasted from other fields like civil engineering, where changes to a design were highly expensive if not impossible (like building bridges), and was wholly unsuited to a world where changes were cheap even after the product had been delivered (like consumer software).

While stressing over the shift to DevOps and the rapid pace of production deployments at Etsy, which made his role as a security gatekeeper particularly difficult, Lackey had a lightbulb moment:

After an embarrassingly long time, I realized this fundamental truth: No matter which development methodology you have, vulnerabilities occur in all of them. But, with its focus on allowing frequent deployments to production, only DevOps gives you the speed to react to those vulnerabilities faster than your attackers.

The methodology of release and rapid iteration was developed to make it easier for software projects to react to what customers really wanted, because often they don't *know* what they want until they have something in front of them.

This applies just as much to security flaws as it does to anything else: unless you have a tiny codebase or the world's best security team, you simply can't cover every possible flaw in testing.

If you're deploying multiple times each day, this at least gives you the agility to fix flaws when they're found, without waiting several weeks for your next deployment or delivering an out-of-band patch.

Security as an enabler... for others to fix their own stuff

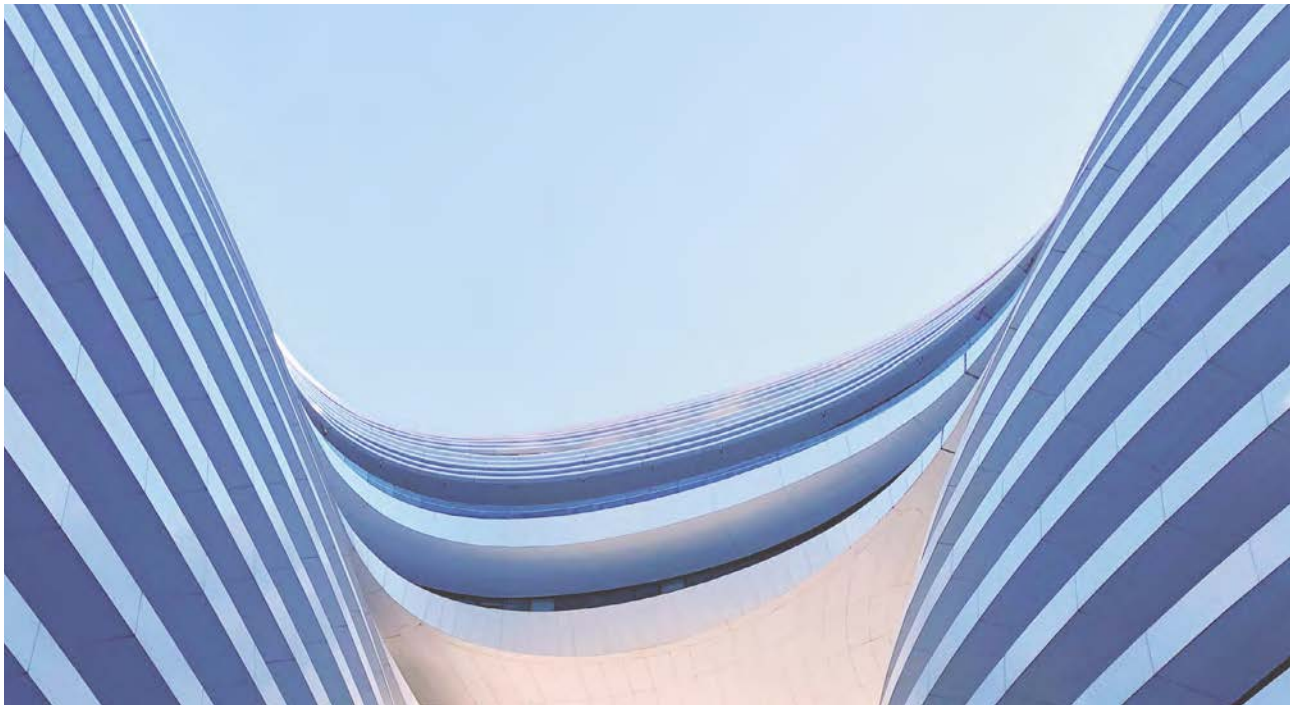
The status quo for security teams is to play whack-a-mole. There's a constant grind to maintain patches and keep ahead of the latest vulnerabilities and misconfigurations - a task made much more difficult when you're also the final hurdle for any new product release. There can be immense pressure on security teams from other areas of the business to wave new releases through. And hey, at the end of the day you're a cost centre.

Lackey also stresses the importance of making the rest of the organisation security self-sufficient, and the role of a modern CSO[3]: *Enable the rest of the business to own their own security.*

In a modern DevOps environment, this works very differently than the example above: the development teams are in control of their own deployments, which includes the security of those systems. In an environment where deployments happen several times a day, this model scales far better than the historical practice of security acting as a gatekeeper to production.

There's an obvious catch to this: your development teams need the skills and tools to secure things properly. This is easier said than done – good developers with security skills are sadly still quite rare.

Even so, you can get a long way with some basic training. To paraphrase Robert Chesney, Director of the Robert S. Strauss Center for International Security and Law[4]: you need developers who are security *literate*, but not necessarily *fluent*.



[3,4] *See Reference List at the end of the report*

Software bugs happen, but if someone messes up a deployment and Netflix goes down, no one dies as a result

Good developers don't want their stuff hacked any more than the security team does. They want to write more secure code, they just need to know where to look, and what sort of attacks they should be expecting. And this means that the job of the security team becomes advising and educating, not gatekeeping.

However... Sometimes, you only get to deploy once

It's important to point out something which is often missed in these discussions: not every software project can or should use modern DevOps approaches.

Sometimes the cost of software flaws is extremely high (failures might be life-threatening), or the cost of pushing a bug fix to production is prohibitive. Often, both are true.

The key benefit of DevOps is that you can deploy rapidly and iterate even after release, which lends itself extremely well to most of the consumer software we use every day.

Software bugs happen, but if someone messes up a deployment and Netflix goes down, no one dies as a result.

This approach is much less appealing for mission-critical software, such as when writing the code for a satellite or an interstellar probe. A software bug might be catastrophic to such a mission, and it's hard to debug a problem and quickly push a new deployment when network communications involve a round-trip-time measured in tens of minutes[5] or even longer (if it's possible at all).

For this sort of project, the famous Facebook motto *Move fast and break things* is *extremely* literal.

Overall, DevOps is a great methodology for shipping consumer software, but it's important to remember that not all software is consumer software. Sometimes, you'll still need the gatekeeper.

EUROPEAN CYBERCRIME CENTRE (EC3)

Europe

Philipp Amann
Head of Strategy

Europol set up the EC3 in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. Since its establishment, EC3 has made a significant contribution to the fight against cybercrime.

What is your biggest cybersecurity concern?

Some of the top-concerns for me are the increasing professionalisation of cybercrime and the convergence of threat actors. A continuously evolving Crime-as-a-Service industry provides the necessary means to commit cybercrime, often giving attack capacity to those otherwise lacking the necessary skills or capabilities. As a consequence, the entry barrier to commit cybercrime is getting lower and allows actors with different motives to launch attacks online.

Combine this with an ever-increasing internet connectivity – often provided through insecure internet of things, the criminal abuse of new and emerging technologies, the borderless nature of cyberattacks, as well as the legal challenges around cross-border cooperation, and you end up with a complex, high cybersecurity risk scenario. Unfortunately, the undeniable advantages and opportunities that cyberspace offers, for instance through new types of connected services, also create a broader attack surface and an asymmetric risk where the actions of few can have a devastating impact on many.

In what areas of cybersecurity do you think we're falling behind?

I think we still have a long way to go in terms of mainstreaming cybersecurity. For industry it is often only an afterthought when developing new products or services. Equally, it is typically not a topic taught at schools – unlike teaching road safety for instance. Organisations need to adopt a culture where cybersecurity is not merely seen as an ICT topic but an integral and essential part of every business process, as well as a shared responsibility across all hierarchy levels.

There is also a need to 'walk the talk' and switch from a predominantly reactive to a proactive response to cyber threats, including prevention and awareness. This requires, among other things, improved sharing of relevant information between various stakeholder groups, including law enforcement, but with a focus – meaning that it needs to be clear what we share, for what purpose and in what format.

What gives you hope for the future of cybersecurity?

GDPR, the NIS directive but also many high-profile cybercrime cases, data breaches and network attacks have created a broader awareness among organisations and individuals of the risks and threats in cyberspace, and the importance of cybersecurity. While there are some unwanted side-effects, new legislation does promote better practices such as security and privacy by design and better cooperation among relevant stakeholders.

At Europol's EC3 we have successfully established public-private-partnerships with organisations who are also willing to add the 4th P – participation. One of the many examples is the No More Ransom project[1], which not only provides awareness and prevention advice but also victim mitigation. The involvement of the public in the context of our Trace an Object[2] campaign also demonstrates what we can achieve together.

I think there is a clear willingness to come together to jointly address current and future cyber threats and to ensure that we can all enjoy the great benefits and opportunities that cyberspace offers. ●

[1][2] *See Reference List at the end of the report*

ARTICLE

EU Getting Serious about Securing Critical Infrastructure

Anne Aune
Security Consultant,
mnemonic

AFTER READING THIS ARTICLE, YOU WILL:

- Understand how the EU is addressing the security of critical infrastructure
- Learn how major national players are working to secure critical infrastructure
- Have an overview of the NIS directive's requirements to Operators of Essential Services

For decades, countries have had security laws regulating how to handle classified information in public institutions, and the physical security of central public buildings and monuments. However, the security of critical infrastructure, especially for private entities, such as air transport, oil and gas installations, or financial market infrastructures, have traditionally not been regulated to the same extent.

That being said, it is not only the private sector that has been overlooked. Even public entities, such as health institutions, water infrastructures, and rail and road infrastructures have in many countries not been subject to security laws. Furthermore, security laws have traditionally lacked a focus on logical security measures, that being the IT mechanisms working as security barriers to prevent or mitigate cyber attacks and human error.

In recent years, we have seen increasing concern about and a renewed interest in the security of critical infrastructure. This is a worldwide concern and there are several examples of nations taking action.

One example is the European Union's efforts to create the *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, also known as the NIS directive.

DID YOU KNOW?

Germany: top of the class

Germany passed the German IT Security Law in July 2015, and was among the first EU countries to ensure security obligations on Operators of Critical Infrastructure (OCI). With this law, OCIs have to implement state of the art technical and organisational security measures and notify the regulator in case of security incidents. In April 2017, Germany also issued the NIS Directive Implementation Act, to ensure full compliance with the directive.

OES: OES include companies and organisations working with infrastructures providing things like food, electricity, water, banking and transport, to name a few.

DSP: Operators of service related to cloud, online market places and search engines, exemplified by companies like Microsoft Azure, Amazon and Google.

THE NIS DIRECTIVE

The NIS directive is an EU and European Economic Area* (EEA) wide legislation that brings forth new security requirements for Operators of Essential Services (OES) and Digital Service Providers (DSP). It is also the first EU-wide legislation on cybersecurity. This article will focus specifically on the security of critical infrastructure, and therefore mainly on the requirements defined for OES. The directive took effect 9th of May 2018, and aims to reach a high and uniform level of security among networks and information systems across the EU/EEA. ▸

EEA: *Iceland, Liechtenstein, and Norway*

Organisations are trying to make informed decisions on security, but have difficulties being truly informed

The difference between a directive like NIS and a regulation like last year's hot topic GDPR is that a regulation is a binding legislative act applied in its entirety, whereas a directive is applied by harmonising national laws with the new directive. In other words, the NIS directive has been interpreted into national legislations by all member states of the EU/EEA. This ultimately means that the way countries meet the NIS directive might be different from country to country. This is likely to become a headache for multinational businesses operating essential services, as specific security measures might be sufficient in one country, but not in another.

Defining Operators of Essential Services

By the end of last year, the EU and EEA countries worked on defining which assets and infrastructures to be subject to their security laws. The NIS directive specified the due date 9th of November 2018 to identify what organisations would be considered OES.

The NIS directive includes high-level requirements on things like security standards and structures. However, it does not specify how an OES should fulfil these requirements in practice. The majority of the EU/EEA countries are now updating their national regulations and making guidelines on how to comply with the directive. In many cases, as a direct response to demands from operators having been defined as OES, that are uncertain about what to do next.

DID YOU KNOW?

The United Kingdom offers compliance guidance

The National Cyber Security Center in the UK has developed a Cyber Assessment Framework (CAF), giving guidance to organisations in the UK that are subject to the NIS directive on what specific measures they need to take in order to comply with the directive.

REQUIREMENTS

The NIS directive emphasises that OES should be subject to national security laws.

The NIS directive requires countries to:

1. Define security requirements ensuring *confidentiality*, *authenticity, integrity* and *availability* of information, and evaluate information systems controlling or supporting essential services

2. Define a national security strategy that, among other things, emphasises cooperation between private and public sectors

3. Implement nationwide Incident Response Teams (IRTs) that can share relevant threat intelligence information with entities subject to national security laws, and that can cooperate across EU borders

4. Ensure that the security measures put in place match the risks the individual OES faces

Defining security requirements ensuring confidentiality, authenticity, integrity and availability

In line with the general trend of digitalisation, OES also aim to benefit from cost-efficient processes, remote operation and maintenance, real time data analytics and improved safety mechanisms. Unfortunately, in order to achieve these benefits, we observe that critical infrastructures have been connected online without sufficient focus on security. By connecting essential services online, new risks concerning confidentiality, authenticity, integrity and availability have arisen.

Security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

- NIS Directive, Article 3 (2)

Security requirements of essential services have typically included how to physically secure assets to ensure their integrity and availability. However, the reality today is that by means of exploiting data, one could also compromise integrity and availability of these services without physical access. For instance in a scenario where a threat actor changes the temperature or pressure levels at an oil platform through gaining access to a control system. Hence, the scope of security requirements must also ensure the logical security of essential services and the systems controlling or supporting the essential services.

The logical security requirements found in traditional security laws have mainly focused on confidentiality of classified information. For critical infrastructure, these requirements might not be sufficient, and sometimes not even applicable.

National cooperation between private and public sectors

Every member state is required to develop a national security strategy which, among other things, *identifies measures relating to preparedness, response and recovery, including cooperation between the public and private sectors.*

The NIS directive emphasises that cooperation between private and public sectors is essential. OES can either be privately or publicly owned, and in some cases have mixed ownership. Complex ownership structures and outsourcing of services make it challenging to establish a uniform level of security for the total value chain. With public entities being dependent on private organisations, and vice versa, the NIS directive emphasises that cooperation between private and public sectors is essential.

DID YOU KNOW?

Norwegian cyber cooperation

The Norwegian National Security Authority (NSM) established a National Cyber Security Centre in the autumn of 2018. The centre assists in protecting basic national functions, public administration and businesses against cyber attacks. To effectively do so, the centre will cooperate with the private sector, the police, national intelligence, academia and international partners.

National Incident Response Teams

Threat actors have broadened their scope on what type of victims and assets they are targeting. We are seeing an increased interest from advanced threat actors in also targeting essential services in order to weaken a country's security. This can either be by attempting to cause major physical damages, or to gain insights about economic market leaders technically ahead of the game or organisations managing classified information. To manage these threats, the NIS directive states that countries should have nationwide Incident Response Teams (IRTs), which should cooperate between public and private institutions as well as between member states in the EU/EEA.

Security measures matching the risk

When countries now renew their security laws and regulations, many look to international best practices on how to manage security. A widely used standard such as the ISO 27000-series points out the importance of having an Information Security Management System (ISMS). The ISMS ensures that organisations make informed decisions on what security measures to implement based on relevant risks. ▸

Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed. - NIS Directive , Article 14 (1)

However, many organisations struggle to evaluate their own security risks – especially because they need relevant knowledge about the threat landscape. Organisations looking for relevant threat information might struggle gaining that knowledge, as information on security breaches are not commonly shared. The outcome is that organisations are trying to make informed decisions on security, but have difficulties being truly informed. To seal this knowledge gap, many countries are now creating secure arenas for sharing information on relevant threat assessments.

DID YOU KNOW?

Norwegian Security Act

On the 1st of January 2019 Norway enforced a new security act addressing the challenge of information sharing by including a law requiring the Norwegian National Security Authority (NSM) to facilitate access to relevant information about the threat landscape to organisations subject to the Norwegian security law.

FINALLY GETTING SERIOUS ABOUT SECURING CRITICAL INFRASTRUCTURE

The NIS directive is a milestone creating a cross-national standard for security in Europe. With it, EU and EEA countries will finally regulate large parts of their critical infrastructure that previously have been overlooked.

As I've touched upon in this article, it has the potential to improve cooperation between private and public entities, include more relevant actors into national security laws, as well as advance the management of threat intelligence and incident response in Europe.

However, it is important to keep in mind that the directive now provides many new actors security requirements that are completely new to them. We are yet to see how this will turn out in the end, and if these changes will have a large enough effect on the actual security of critical infrastructures.

Regardless, the NIS directive is the starting point of when the conversation about securing European infrastructure got serious. If you're like me, you'll be holding your breath to see what 2019 will bring, and what the effects of the NIS directive will mean for the future of security in Europe. ●

The Netherlands

ROYAL SCHIPHOL GROUP

Wilma van Dijk
CISO and Director of Safety, Security & Environment

Royal Schiphol Group is an aviation company. Schiphol offers high-quality air traffic facilities and ensures that their airports are optimally accessible. Their ambition is to remain Europe's Preferred Airport for all travellers, airlines and logistics service providers.

What is your biggest cybersecurity concern?

One of my major concerns is the security of objects, particularly as we continue to move towards more 'internet of things' (IoT). Many devices are not properly secure in their current state, and this poses a threat to our general digital domain. The Mirai-botnet, which consisted of hacked IoT devices, gave an important warning about this. Needless to say, there are secure devices but they are the exceptions to the rules. This lack of security can hinder the growth and acceptance of these technologies. I hope the industry can take a step forward in improving cybersecurity standards and best practices for IoT technologies in order to protect users.

In what areas of cybersecurity do you think we're falling behind?

Most organisations are part of a digital ecosystem, and these digital connections provide opportunities. At the same time, they provide possible attackers multiple 'access points' into organisations. This means that an organisation can still be vulnerable, even if it is highly secured. In other words, a digital chain will only be as strong as its weakest link.

One solution is found in collaboration across organisational boundaries. If we in the Royal Schiphol Group know our interdependencies and weaknesses, we can create a safe and strong airport ecosystem with direct trusted connections to various partners. Schiphol began the *Cyber Synergy Schiphol Ecosystem (Cyber Synergie Schiphol Ecosysteem, or CYSSEC)* initiative in 2017, in order to invest in cybersecurity awareness, as well as to join forces to keep our ecosystem secure and reliable.

What gives you hopes for the future of cybersecurity?

There are some good news: higher security standards are becoming the norm, even as new threats and technologies become more complex. It seems like cybersecurity is no longer an obstacle standing in the way of change within organisations. In fact, it is an enabler and often a basic requirement for digital transformation and innovation. Despite the focus on technology, appropriate cybersecurity measures still require cyber experts and 'cyber aware' people, because in the end, people make the difference in winning the 'cyber game'." ●

ARTICLE

Agile Security Strategy

Angel Alonso
Senior Security Consultant,
mnemonic

AFTER READING THIS ARTICLE, YOU WILL:

- Learn how to create a security strategy that can adapt to changes in your environment
- See how security can help you reach your organisation's overarching goals
- Understand the benefits of challenging some of the established conventions regarding security strategy

Are you familiar with the cartoon "and in this corner we have Dave"? Surely you know the picture. A boxing ring, and in one corner you have firewall, encryption, antivirus software, etc.; in the other corner you have Dave, a middle-age man wearing a t-shirt with the text *Human Error*. I often cringe when I see this picture used in presentations like user training, as it represents an outdated mentality. Can we really just blame users anytime our security controls fail? It's certainly not that black and white.

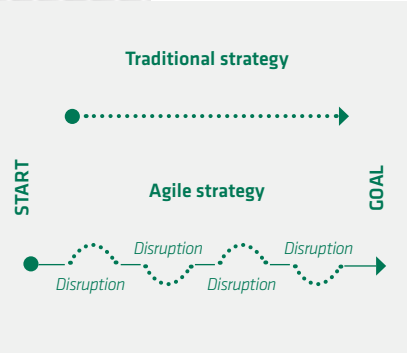
An encouraging trend we are seeing however, is that more organisations are enabling and working with their users, rather than blindly using them as a scapegoat. This isn't the only mentality shift we're seeing amongst organisations. In my position in the Governance Risk & Compliance (GRC) department in mnemonic, I often work as a CISO for hire. This has allowed me to be part of many shifts like these, where organisations mature by acknowledging new realities, make use of new technological advances or are simply being forced to adapt to disruption or legislative changes in their environment.

Another change I've observed over the past years is that mature organisations are to a lesser degree looking to prevent all security threats. Rather, they are shifting their mind-set to acknowledge that security incidents will happen. So in addition to preventing security threats where possible, they are adopting a balanced approach putting emphasis on detecting and responding to threats that will bypass preventive controls. Then there is the development that puts the biggest smile on the faces of people in my position. The CISO is now much more often invited to and involved in the boardroom. It is a positive sign that security is being discussed at the very top levels. While it does not always translate to increased investments, it is certainly a positive trend that it's part of the conversation.

Listing the changes I, and many CISOs with me, have seen over the last years could be an interesting exercise in itself. However, what I find most interesting is what these shifts can teach us about creating a mature, lasting security strategy.

A new approach

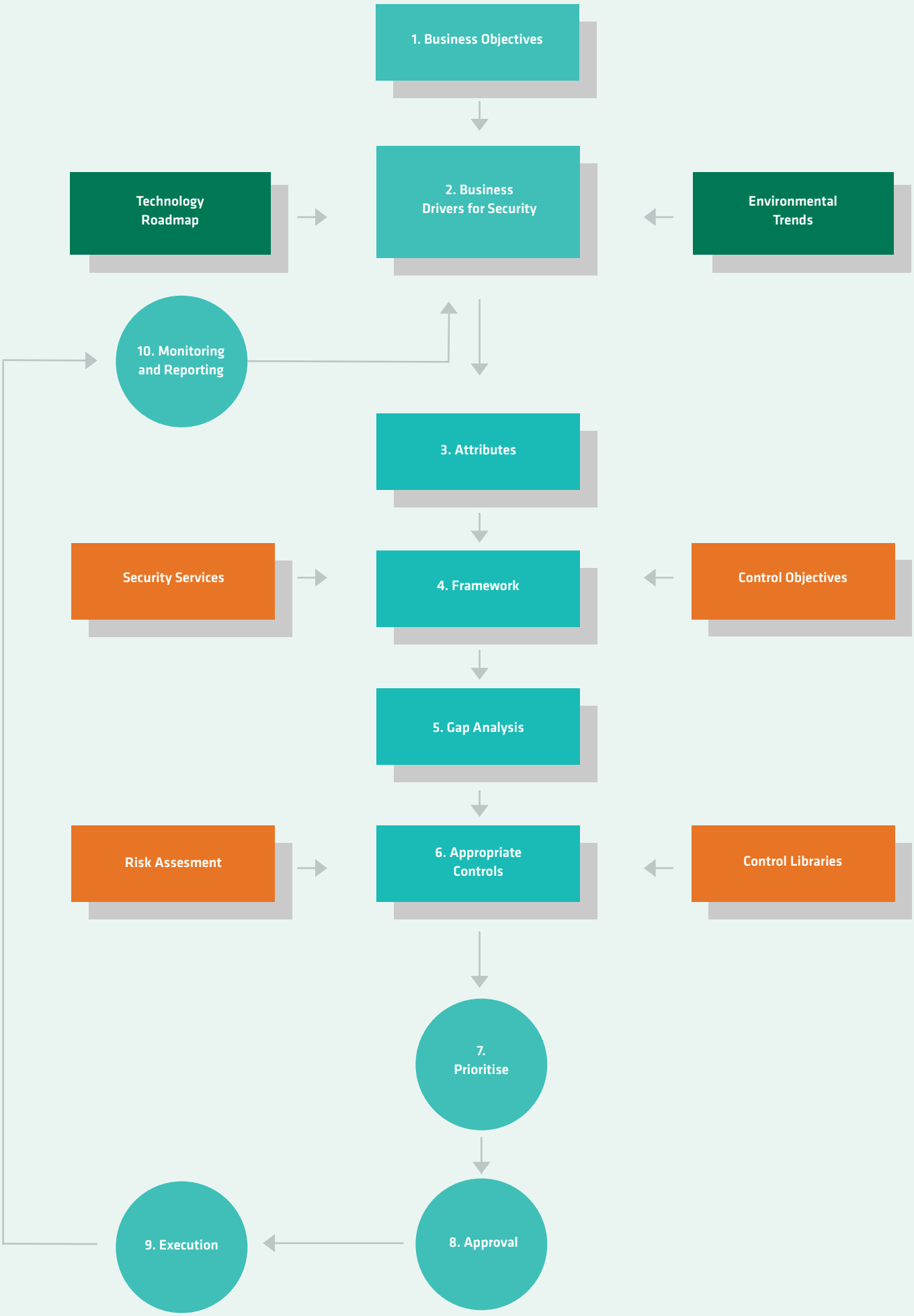
What disruptions, technological advances, learnings or legislative changes will affect your organisation in the future? This is not an easy question to answer. Yet at the same time, you, your team and your Board are tasked with developing a security strategy for the next three, four, even five years.



How can we create a security strategy that won't become obsolete as soon as the ink touches the paper? If we want to adapt to what is happening around us, we need to move away from the traditional, linear way of looking at strategy. It cannot be a static document that hopefully predicts your organisation's next three years of security challenges. If a security strategy is to survive under these uncertainties, it has to be able to adjust according to the changes in your environment.

One way of doing this, and what I often aim to do in my work, is to create strategies that from the start facilitate for short interval review, reconciling with current realities while pursuing our business goals. Both the SABSA framework[1], and Gartner's report *Develop a Pragmatic Vision and Strategy for Digital Business Security*[2] are great resources for this exercise. In the following chapters I will use these resources to present how to make an *Agile Security Strategy*. ▸

[1,2] *See Reference List at the end of the report*


1. Business Objectives
2. Business Drivers for Security
Technology Roadmap
Environmental Trends
10. Monitoring and Reporting
3. Attributes
Security Services
4. Framework
Control Objectives
5. Gap Analysis
Risk Assesment
6. Appropriate Controls
Control Libraries
7. Prioritise
8. Approval
9. Execution

A MODEL FOR MODERN SECURITY STRATEGY

To build a security strategy that can adapt to the shifts in the environment we live in, we need to move away from traditional linear security strategy models and adopt more dynamic, agile models. In theory, an agile model can look something like the model to the left. On the next page you will see what this model could look like in practice.
We start off by identifying our organisation's business objectives.

1. Business Objectives

In other words, what your organisation would like to achieve. It's important to keep in mind that our security strategy should be business-driven, so that it enables us to support the organisation's long-term business objectives. It should definitely not work against it.

2. Business Drivers for Security

Then, you identify your Business Drivers for Security. This step is the link between business and security, and is where we define what the security team can do to help achieve your organisation's business objectives.

Defining what and how many Business Drivers for Security you want to include in your strategy should be based on the needs of your organisation. Factors like the need for cost reduction, modularity, scalability, ease of component re-use, operability, usability and inter-operability are expected to play a part here. Therefor this step needs to take into account the company's technology roadmap and be aware of external environmental trends.

Both this and the step above belongs on the higher management level, and in-depth security knowledge is not necessary to identify these two steps.

3. Attributes

At this point you ask yourself; how can the security team actually achieve what we have defined in the two steps above?

To answer that question we identify a set of attributes, which will measure performance in a way that is understandable for all stakeholders.

4. Framework

We've gotten this far on our own, and now it's time to get some help. The first three steps are highly individual to your organisation, but the framework you choose to support your attributes does not necessarily have to be. You do not need to reinvent the wheel on this one. There are plenty of existing industry-accepted standard frameworks out there that you can easily adapt to your situation.

The framework you choose here defines how the rest of your process will continue on, and how we reach and support our attributes through security services and control objectives.

5. Gap Analysis

Once we have defined our framework and what it is supposed to achieve, we analyse the gap between our current situation and our business objectives.

6. Appropriate Controls

From our framework (standard or not) we will be presented with many different controls that will help us support our attributes. The findings from our gap analysis will also highlight what controls are missing.

7. Prioritise

We will probably not be able to start all activities needed to implement the appropriate controls at the same time. At this step we therefore need to prioritise where to start. I recommend taking a risk-based approach, prioritising based on the current risks that we are facing, and the impact and likelihood of these risks.

8. Approval

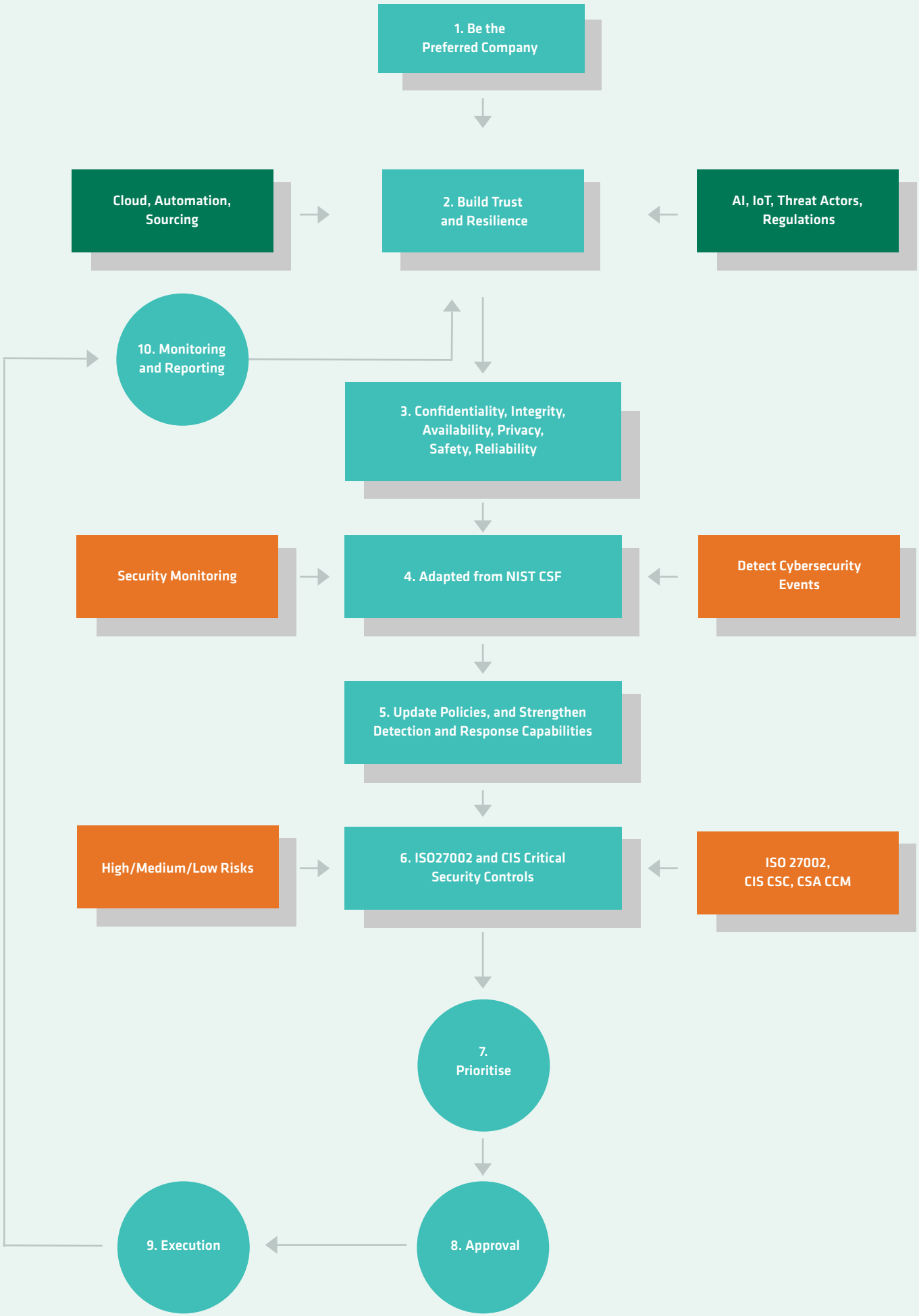
You then present your work so far to management. Your goal is then both to make them understand the risks your organisation faces, and commit to supporting your approach with the necessary resources.

9. Execution

Now, you can begin the execution phase.

10. Monitoring and Reporting

You need to follow the arrowed lines in the model and come back to this step regularly to be able to detect and adapt your strategy to shifts and changes, as well as to ensure continuous alignment with the Business Drivers for Security. This way you will close the cycle for the agile security strategy. ▸


1. Be the Preferred Company
Cloud, Automation, Sourcing
2. Build Trust and Resilience
AI, IoT, Threat Actors, Regulations
10. Monitoring and Reporting
3. Confidentiality, Integrity, Availability, Privacy, Safety, Reliability
Security Monitoring
4. Adapted from NIST CSF
Detect Cybersecurity Events
5. Update Policies, and Strengthen Detection and Response Capabilities
High/Medium/Low Risks
6. ISO27002 and CIS Critical Security Controls
ISO 27002, CIS CSC, CSA CCM
7. Prioritise
9. Execution
8. Approval

THE MODEL IN PRACTICE

Let us now view the model in practice. I believe many organisations could recognise themselves in a model filled in like this:

1. Business Objectives

The business objective we set for this fictional company is something as general as "to be the preferred company for its customers".

2. Business Drivers for Security

Gartner tells us that in order for us to be successful in reaching our goal, we have to inspire trust and build *resilience* between the business and our customers.

These drivers for security will be influenced by our internal information technology strategy (e.g. cloud adoption, degree of automation, sourcing strategy, etc.) and external environmental trends (e.g. disruptive technologies, more sophisticated threat actors, new regulations, etc.).

3. Attributes

To support Business Drivers, the security community have traditionally focused on three attributes often called the CIA-triad: Confidentiality, Integrity and Availability.

However, this is an example of another convention that need change to adapt to the world we live in today. We need to expand the triad to cover requirements that may arise in digital business initiatives where the line between logical and physical security is blurred. Hence, we also need to incorporate the attributes Privacy, Safety and Reliability.

4. Framework

Instead of reinventing the wheel, and engineer a completely new security framework, we adapt the NIST Cyber Security Framework defining four main control objectives:

- Manage security risk
- Protect against cyber attack
- Detect cybersecurity events
- Minimise the impact of security incidents

And a set of security services:

- Governance
- Risk management
- Identity and access control
- Staff awareness & training
- Vulnerability management
- Data security
- Security monitoring
- Response and recovery planning

5. Gap Analysis

Based on our recently established framework we can now conduct a gap analysis between our current state and our target state. This analysis will identify the full set of activities that are necessary to perform. For instance, we can find that we will have to work on our policies, and that we need to strengthen our detection and response capabilities.

6. Appropriate Controls

To address the gaps mentioned above, we select our controls from standard libraries. For our work with policies, we choose controls from ISO27002; and to strength detection and response capabilities, we use the CIS Critical Security Controls.

7. Prioritise

If we cannot begin both control processes at the same time, we then need to prioritise where to start.

8. Approval

We present our strategy-in-process, with the goal of receiving support from the rest of the organisation. Support in this case is a formal approval of the strategy, so we can start bringing it to life.

9. Execution

And then, we implement (sometimes easier said than done, though tips for succeeding with security project implementations warrants its own discussion).

10. Monitoring and Reporting

An agile security strategy does not stop here. It's important that you start reporting on your progress in closing the gap from your analysis. You should reconcile the strategy periodically (for instance yearly or when need be) to ensure you organisation's goals are still in correct alignment with the business.

In this article, I've tried to convey the importance of not looking at a security strategy as a decree that is cast in stone, not to be changed for the lifetime of the strategy, but rather a living document that should be re-assessed and adapted to changes in the environment. And I've tried to convey how I usually solve this challenge in my work.

Now it is your turn to challenge the traditional security strategy approach and put this model into practice in your own organisation! Feel free to visit

www.mnemonic.no/agile-security-strategy

to find additional resources on how you can build *your* agile security strategy.

EQUINOR

Global

Sindre Skjønsberg
Principal Analyst Information Security

Equinor is an international energy company present in more than 30 countries worldwide, including several of the world's most important oil and gas provinces. Founded in 1972 under the name Den Norske Stats Oljeselskap AS – Statoil, they changed their name to Equinor in 2018. Equinor's headquarters are in Stavanger, Norway, and the company has over 20,000 employees.

What is your biggest cybersecurity concern?

The devastating impact cyberwarfare can have on people, organisations and critical infrastructure. Nations have cyberweapons as part of their arsenal, and some have already shown they are both willing and capable of taking down services we depend on in our daily lives. To make matters worse, these weapons are notoriously difficult to control, making them a threat also to organisations or individuals not directly involved in the conflict.

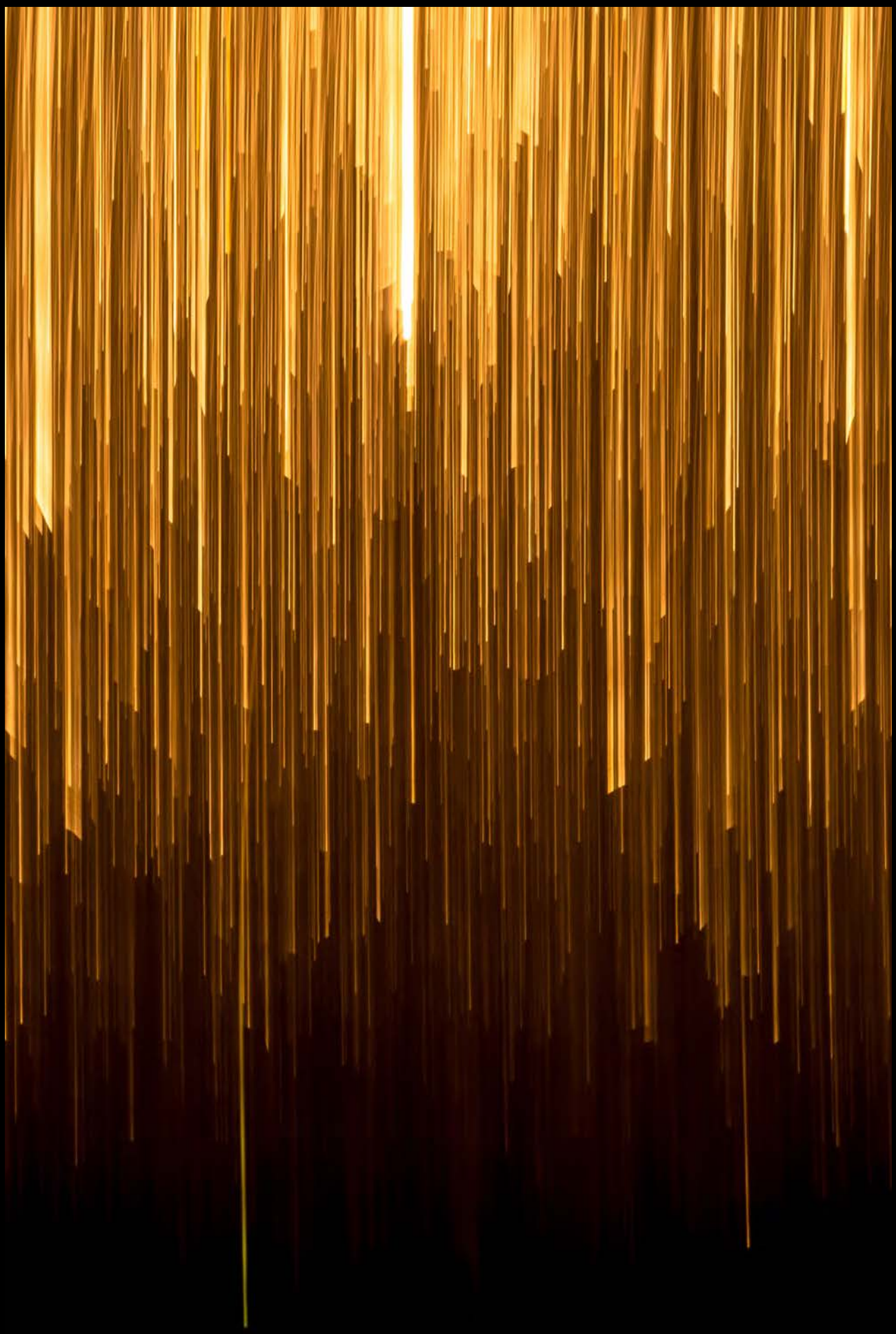
As society is becoming more dependent on IT, the number and scale of such attacks is likely to increase.

In what areas of cybersecurity do you think we're falling behind?

We are failing to close the cybersecurity competence gap, as the demand for qualified personnel appears to outgrow the supply. Part of this stems from the fact that knowledge of cybersecurity is required in all professions, not just within the core security functions such as SOCs and CERTs. On the bright side, there are several initiatives and institutions already working on turning the tide.

What gives you hope for the future of cybersecurity?

That cybersecurity no longer is a topic reserved for IT professionals. Cyberattacks have become front page news and are being discussed in all areas of society – from the average person on the street to the board of directors. The result is a greater interest in cybersecurity than ever before, and we are getting closer to making it a life skill.



ARTICLE

Semi-Automated Cyber Threat Intelligence (ACT)

Making knowledge about threats useful

Martin Eian
Head of Research & Development, mnemonic
Project Manager, ACT

AFTER READING THIS ARTICLE, YOU WILL:

- Learn more about the public-private collaborative platform ACT, and get a crash course in how to operate it
- Understand why the article writer saw the need for yet another threat intelligence platform
- See how to make use of otherwise scattered information about threats and threat actors

Back in 2014, mnemonic's Threat Intelligence team was working on how to solve an escalating challenge: how can we collect and organise our knowledge of threats and make it useful? As a global security service provider, an active member of the security community and through our partnerships, we are presented with an enormous amount of threat data, information and intelligence. While it may sound like a luxury problem, the reality is that if you do not have a structured way to collect, assess, and most importantly, apply this data, it can become more noisy and distracting than useful.

As mnemonic and our customer base grew, so did the amount of data the Threat Intelligence team were tasked with sifting through to structure, evaluate, and apply to our daily operations. As a team we continually evaluated how we could address this challenge, knowing that it would only escalate as time went on. We had our threat intelligence framework in place, we had the processes, and we had the expertise. What we were missing was the technology to support our ambitions and the way we wanted to work with threat intelligence.

So we started mapping out what we actually needed technology to support us with. We needed a threat intelligence platform that could store all our knowledge and make it easy to search and retrieve it when needed. We needed the ability to automate, where possible, the manual work that our analysts spent their time on. We needed the ability to share information, not just data, and to automate countermeasures. We needed new methods and mechanisms for enrichment and analysis. We needed a platform that was scalable, that supported strict access control, and that was easy to integrate with existing systems.

If you can't buy it, build it yourself

After mapping out our requirements, we hit the open market to find a platform that would support our needs. This included speaking with our colleagues in various security agencies, private sector, CERTs, and so forth to find out how they were tackling these challenges. It became apparent rather quickly that the platform we, and others, needed simply didn't exist. So if you can't buy it, the next best option is to build it yourself.

Realising we weren't alone in this need, we teamed up and sought external funding for an innovation project to develop a new, cutting-edge threat intelligence platform that would not only solve our challenges, but something we could make open source to help solve the challenges of organisations globally. Together with the Norwegian National Security Authority (NSM), the Nordic Financial CERT (then FinansCERT), KraftCERT, the University of Oslo (UiO) and the Norwegian University of Science and Technology (NTNU), we submitted an application to the Research Council of Norway for funding a three year project. ▸

In 2016, our application for funding was approved, and after a short ramp-up phase, the *Semi-Automated Cyber Threat Intelligence (ACT)* project went full speed ahead from January 2017. In 2018, Telenor joined the project as well.

This article will summarise the progress, major achievements, and roadmap as we enter the third and final year of the project.

The underlying data model

One of the first obstacles we tackled was to develop a data model that supported our needs. We needed a model that could express complex information in a machine-readable manner, and at the same time present understandable information to human analysts. The result is a model with two components: objects and facts.

Objects represent "things", something that exists independent of the information that we have about it. Examples of objects include IP addresses, domain names, file hashes, email addresses, reports, persons, groups, threat actors, tools, tactics, techniques, procedures, sectors, locations, and campaigns. In our data model, objects have no properties other than their value, so for example 127.0.0.1 for an IPv4 address.

Facts on the other hand represent information about objects. A fact can be connected to:

- a single object
- two objects
- a single fact

Facts are immutable, so they cannot be deleted or modified after they have been added to the platform. If a fact later turns out to be incorrect, a new fact can be added to retract the erroneous fact. Facts are also timestamped. The combination of immutability and timestamps makes it possible to "rewind time": to see exactly what information was available at any previous point in time.

Facts also support access control, both role-based and explicit, and every fact has an owner. In order to access an object, the user must have access to a fact connected to it. Every fact has a source that describes where the information came from, and facts can be linked to evidence supporting the fact.

Only facts can be added to the ACT platform. Objects are added automatically when a fact connected to it is added. The rationale for this is that adding an object on its own is not useful. For example, adding an IP address without any kind of context provides no value. The platform forces users to explicitly state why that IP address is of interest by creating facts connected to it. This also facilitates information sharing, since sharing facts will recreate the exact same information in the recipient platform, as opposed to sharing methods that lose information.

Another advantage of the data model is that objects are unique. If you search for an IP address, then you will immediately find all recorded information about that IP address.

To implement the data model, we defined object types and fact types. One example fact type is the DNSRecord fact:

This fact uses information from the Domain Name System (DNS) to connect fully qualified domain name objects (FQDN) to IPv4 or IPv6 objects. The meaning of this fact is that a domain name has resolved to an IP address.

The implementation of the data model is still a work in progress, and we add new object types and fact types as they are needed. It is also possible for users to define their own object and fact types in their own implementation of the platform, as well as share these definitions with others.

Visualising data with graph queries

When implementing the data model, we quickly realised that we needed to be able to represent it as a graph. Graph representation enables graph queries, which facilitate powerful analytics.

Objects represent nodes in the graph. Facts connected to a single object represent node properties. Facts connected to two objects represent edges. Finally, facts connected to a single fact represent edge properties.

In order to support graph queries, we implemented the low level Blueprints API from Apache TinkerPop, an open source graph database stack. The API lets us use the rest of the TinkerPop stack, including the Gremlin graph query language and graph traversal strategies. Furthermore, we enforce access control in our API implementation, so in essence we have built an open source, scalable graph database with strong access control. This graph database could be used for other applications as well, but we use it as a threat intelligence platform. ▸

The power of graph queries is best illustrated by a few examples.
As a SOC analyst, I receive an alert on suspicious traffic towards an IP address. I query the address using the ACT platform and get the following result:

This screenshot shows what we know about three domain names (FQDN objects represented by the red circles) that have pointed to the IP address (ipv4 object represented by the blue circle). This is recorded as DNSRecord facts.

This in itself has limited value to me as an analyst, but if I can start expanding the domain name objects to find other facts connected to them, things start becoming more interesting. These associated facts tell us other information about the domains. If this information (facts) is connected to other objects, we can start gaining more context about the domains. For example one would expect that these connected objects could be threat actors who used the domain in the past, associated campaigns, reports mentioning the domain and so forth.

Manually expanding, drilling down and digging to find potentially useful information could become a time-consuming task. A graph query automates this process.

As an example, let's say I want to learn which published threat intelligence reports have mentioned domains associated with the IP address in question. I can use a query to find all FQDN objects connected to the IP address, and then find all reports that mention those domain names.

This quickly shows us that there are quite a few reports mentioning the three domains associated with the IP address in question. Furthermore, we can see only a single report mentioning two of the domains (the green circle connected to two red circles) – so perhaps this is the report we should look at first.

Now we of course know that domains can change the IP address they are pointing towards, and that attackers often re-use their infrastructure. So we incorporate this into our query by also including other IP addresses that have at some point been associated with the three domains in our original query. We also include the domains associated with these other IP addresses, and the IP addresses associated with these new domains, and so on.

We can control the query to go six levels deep (as in ipv4-fqdn-ipv4-fqdn-ipv4-fqdn-ipv4), and show all reports mentioning any of the IP addresses or domains produced in the query. For good measure, we can also exclude all known sinkholes from these results.

The result looks like this.

While this result is not very readable in a document, it demonstrates how a basic query starts painting a bigger picture of associated information related to a specific IP address. The platform's interface is interactive, enabling analysts to zoom in, expand objects, add filters, change graph layouts, step back through their search histories, and export their search histories. The graphical user interface (GUI) is built on top of a representational state transfer (REST) API.

The API also serves other purposes, such as process automation. ▸

Automation

One of our primary goals with the ACT project is to automate otherwise time-consuming manual tasks, where appropriate and possible. After an extensive search for workflow management systems, we selected Apache NiFi[1], which allows us to define data flows to and from the ACT platform.

In addition to NiFi, we have implemented workers that communicate with the ACT API and external systems. The workers can import information, enrich data, export infor-mation, perform analysis or trigger countermeasures. In other words, facilitating for analysts to be able to spend their time where it really matters.

To facilitate the development of workers, we developed a Python library that makes it easy to interact with the ACT API directly from Python. A Splunk app has also been developed to facilitate integration with Splunk, making it possible to query ACT data and annotate search results, all within Splunk.
So far, we have implemented several workers, including:

- MITRE ATT&CK import worker[2]
- MISP Galaxy import worker[3]
- MISP feed import worker
- Scio import worker
- mnemonic PassiveDNS enrichment worker[4]
- VirusTotal enrichment worker[5]

Bootstrapping

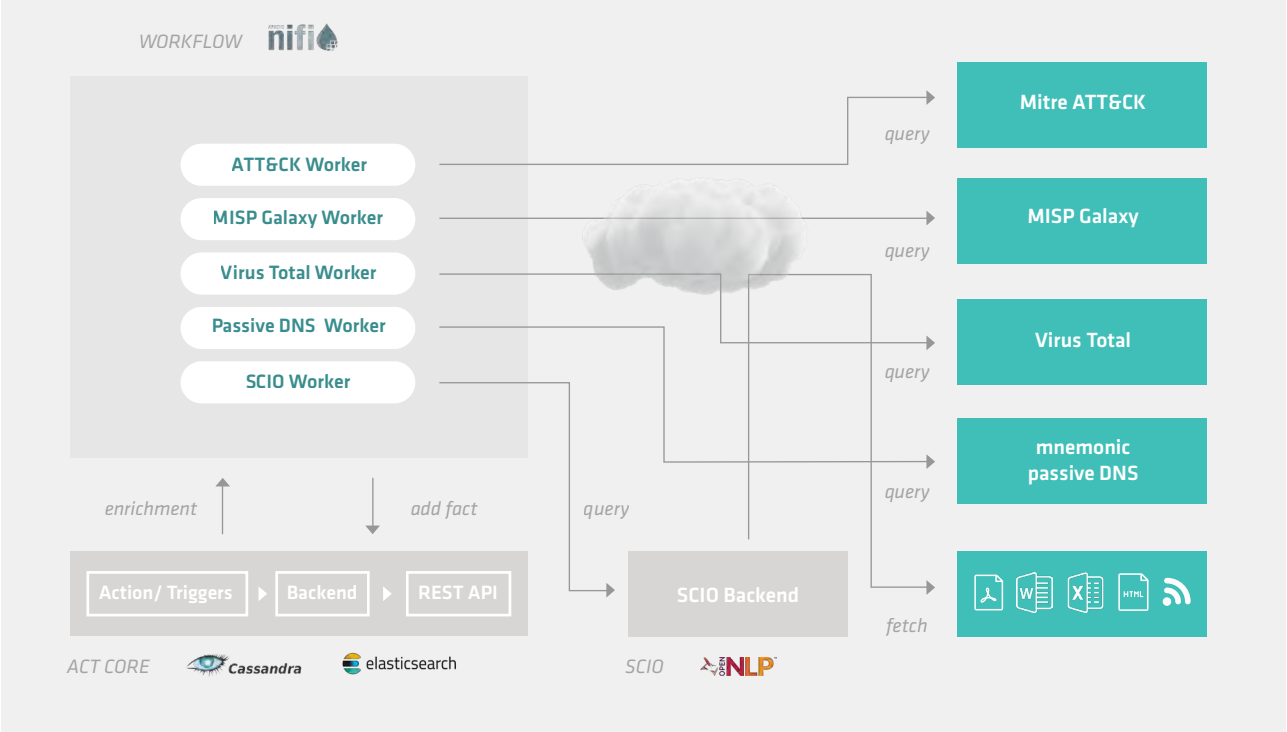
To test and validate the platform, we required large amounts of threat information. Most of the openly available threat information is unstructured, human-readable text - commonly in the form of reports and blog posts. We therefore developed *scio*: a system that uses natural language processing, pattern matching, and ontologies to extract structured information from human readable text.

Scio continuously downloads new threat reports and security related blog posts, extracts structured information from them, and adds this information as facts to the ACT platform. The enrichment workers automatically add more context. For example, if we observe a file hash in a report, then the VirusTotal enrichment worker will find malware family names and command and control infrastructure from VirusTotal, and then add facts connecting these to the file hash.

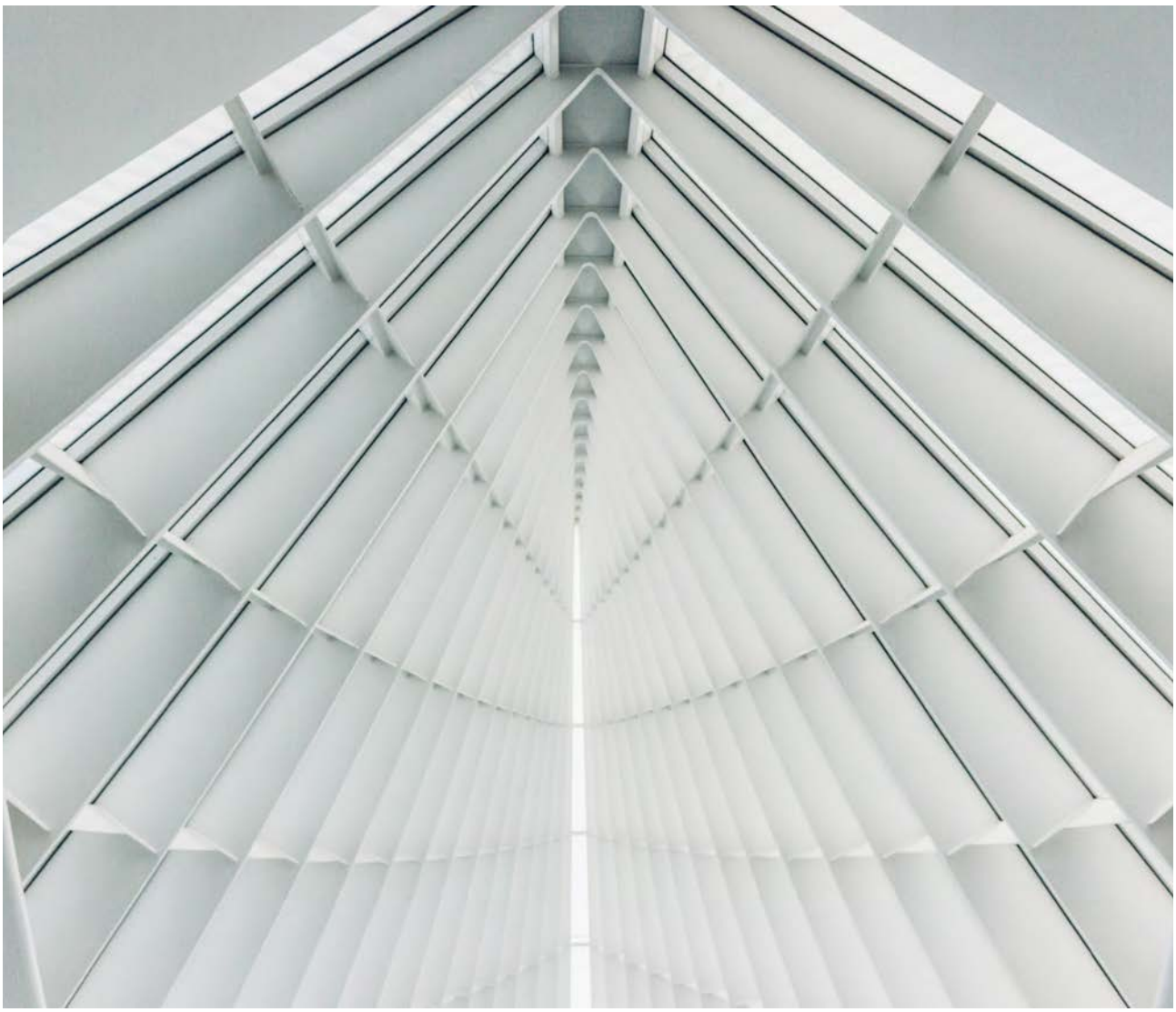
Overview

Each and every one of the topics mentioned in this article could have been an article in itself, but as the article now comes to an end I hope you are left with an overview of the ACT platform and some of its most important functionality. The figure below illustrates how all of the different platform components mentioned throughout the article interact:

Interaction between Platform Components



[1][2][3][4][5] *See Reference List at the end of the report*



Future work

As the ACT research project continues into 2019, the roadmap is set to improve out-of-the-box functionality related to flexibility, usability, automation and interoperability. This includes:

- Major GUI improvements, including timelines
- Automated analytics
- Quantifying trust (information sources) and confidence (facts)
- Lossless information sharing between ACT platform instances
- Automated countermeasures
- More workers, including STIX import/export
- Revised and extended data model implementation

Want to know more?

The ACT source code is published under the ISC open source license on Github:
github.com/mnemonic-no/

If you would like to test the platform, we have a publically available read-only ACT platform instance on Amazon AWS:
act-eu1.mnemonic.no/

We have presented hands-on ACT workshops at the 30th FIRST Conference (2018) and the Oslo FIRST Technical Colloquium 2018. Our next workshop will be at the FIRST Cyber Threat Intelligence Symposium 2019 in London on March 18th: www.first.org/events/symposium/london2019/

Last, but not least, please reach out to us if you have questions or if you would like to contribute to the open source ACT project.

2018: A VIEW FROM MNEMONIC'S SECURITY OPERATIONS CENTER

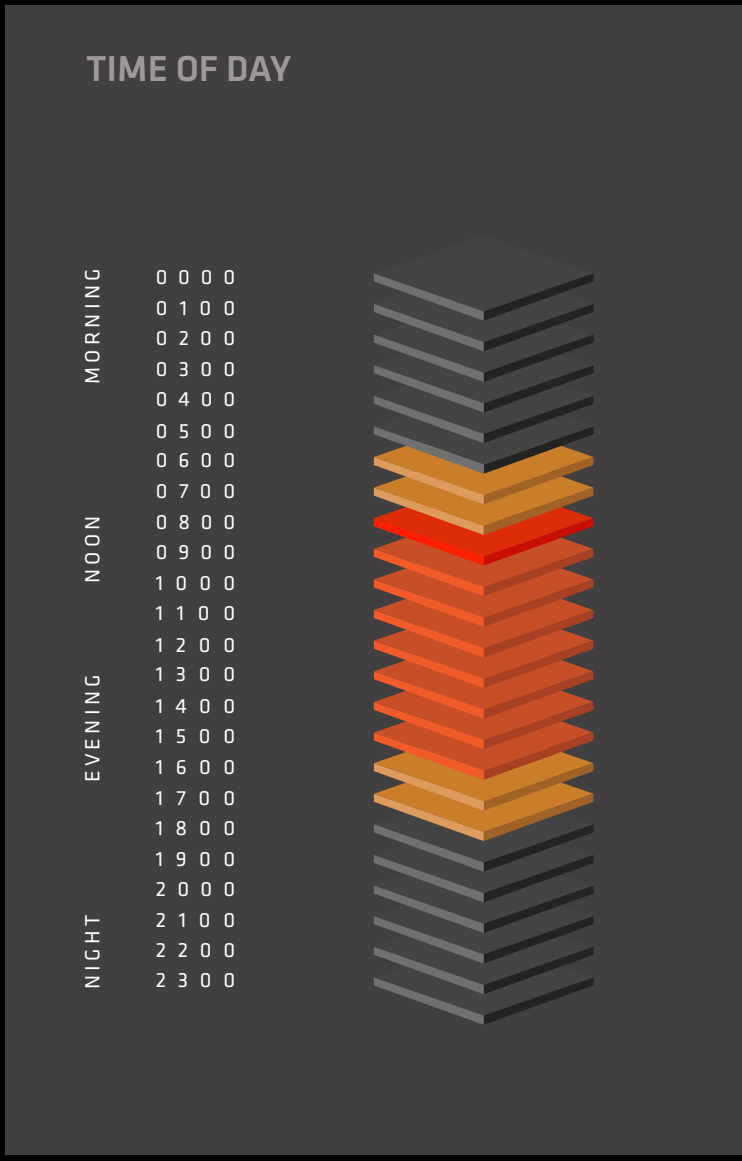
All statistics are from real customer cases detected from our Security Operations Center

WHEN ARE SECURITY INCIDENTS HAPPENING?

TIME OF DAY

It is no surprise that security incidents happen during all hours of the day. However, as we have observed in previous years, the number of incidents increase between 08 – 16. This increase during business hours supports the established truth that more user activity tends to lead to more security incidents.

In last year's report, we observed that the volume of incidents were spread evenly throughout the most common working hours of the day. Our numbers from 2018 show that this is still the case, but with a noticeable peak in the morning when most people start their work day. This could perhaps be because users are being infected at home and it then only being detected when they connect to the corporate network, or because users in the morning quickly go through their email from the night before and hence is more likely to inadvertently click on something they shouldn't.



60%

Consistent with our observations in previous years, 60% of security incidents across all severity levels occur during the office hours of 08 – 16 on weekdays. In other words, security incidents are occurring at all hours, but there is a definite correlation between the workweek and when users are most active, and the volume of security incidents occurring.

77%

77% of targeted attacks occurred during the business hours of 8 – 16 on weekdays. This coincides with the patterns we see through our incident response engagements in how targeted attacks occur – namely that users most often serve as both the target and an enabler for the initial compromise in these attacks.

SEVERITY OF INCIDENTS

Looking back the past three years, we have seen a noticeable increase in the ratio of Low severity incidents as compared to all incidents observed. From the beginning of 2016 to the end of 2018, the ratio of Low severity incidents has increased by 30%. On the flip side, the ratio of High severity incidents has decreased by 80% in the same time period.

This relatively large drop in High severity incidents does not necessarily indicate that High severity incidents are not happening. The reality is that 2016 in particular was a busy year for encrypting variants of ransomware, thereby inflating the numbers for that year. This returned to morepredictable numbers in 2017, and in 2018 we saw a significant shift towards less destructive ransomware iterations as attackers move to tactics like coin mining, which are often seen as Low severity by customers.

WHAT DAYS ARE SECURITY INCIDENTS HAPPENING?

Users are more likely to be involved in a security incident during the workweek, and this is most likely to happen earlier in the week. The first day back after the weekend is statistically when most incidents tend to take place. Similar to the per-hour incident trends, the most likely explanation for this increase is a combination of users returning to the office after the weekend with their laptops, which have been infected outside of the corporate network, and users quickly moving through a weekends' worth of emails when they first return to the office and being less aware of the actions they are taking.

TIME OF WEEK

05%
SATURDAY

05%
SUNDAY

28%
MONDAY

13%
FRIDAY

15%
THURSDAY

17%
TUESDAY

17%
WEDNESDAY

WHEN ARE USERS BEING INFECTED?

Our observations show that systems were more frequently *exposed* to malicious code bright and early in the morning - around 8 o'clock. This is likely because this is when many start their day at the office, logging into laptops, looking through their email, or perhaps having a soft start by browsing or even doing some personal activity online, like checking social media.

Exposure to malicious code in itself does not represent a successful infection. *Successful* malicious code infections however, statistically peak between 10-11 o'clock. In past years, we have seen successful infections peak during lunch hours. Why this has shifted an hour earlier is pure speculation on our part. Perhaps low blood sugar before lunch is to blame?

ARTICLE

Serverless Security

Andreas Claesson
Senior Security Consultant,
mnemonic

AFTER READING THIS ARTICLE, YOU WILL:

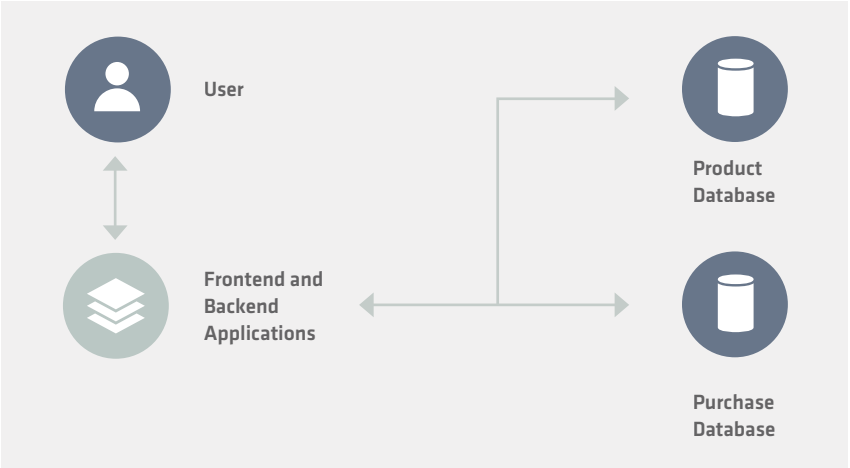
- Learn about the benefits and drawbacks of serverless security
- Understand how serverless security is challenging traditional IT security
- See how these challenges can be mitigated

The world of IT is changing, and more and more services seem to be moving from centralised servers to decentralised server providers, i.e. cloud vendors like Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). The services themselves are also becoming more decentralised, meaning that they are broken down into smaller pieces called *microservices*. Common examples of microservices are AWS S3 buckets for storing objects in the cloud, and AWS Lambda for running small pieces of code. Several microservices are then interconnected in order to provide the original functionality of the service it replaces.

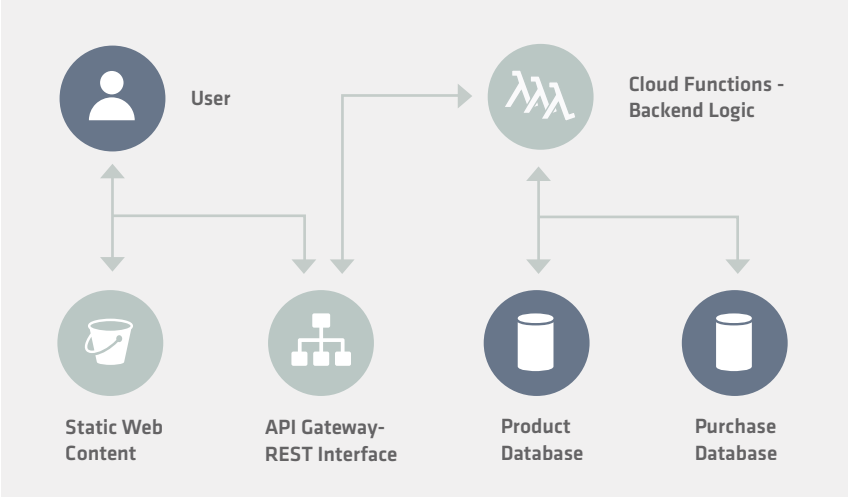
Let's look at an example. Imagine a standard web application, say an online store selling products over the internet. You would have the web application itself, a product database for all your goods, another database (with higher protection) for storing all transactions and potentially sensitive information like credit card information, and maybe other connections to various backend services. Then you would have some kind of backend server software to orchestrate everything.

All these pieces of the application could be implemented as a separate microservice of its own, and the backend server software could be broken down into separate functions each with their own specific task. You have one specific function that handles searching the product database only, and another function for placing orders, and so on. This way of architecting applications is called *serverless*, and is rapidly becoming the standard by which companies develop new services and applications. ▸

Traditional Environment



Serverless Environment



From a security perspective, this offers a quite dramatic change in how we look at securing our applications. First of all, there is no real perimeter as defined in traditional IT security terms. Instead, all microservices have their own environment that has to be secured with policies, roles, audit trails, etc. This vastly increases the attack surface, and introduces a whole new way of looking at what needs to be secured and how.

This article will look into a few of the most important aspects of serverless security, and explain the most critical areas where special attention is needed. It will also discuss some common misunderstandings about the perceived security in some of the microservices.

FROM MONOLITHIC SERVERS TO SERVERLESS VIA CONTAINERS

Transforming an application that runs on traditional servers to a serverless architecture can be a daunting task. In fact, in many cases it would be easier to rewrite the whole application from scratch rather than trying to redesign it. Especially if the application is large with a lot of functionality. However, if the goal is to migrate from on-premises servers to a cloud solution, there are some ways to run legacy applications in the cloud without too much redesign.

Virtual servers provide a quick and easy way to move existing on-premises systems to the cloud, but the main benefits such as scalability and cost improvement, will be lost. An interesting approach when preparing for the cloud is to break down the applications in individual parts. These parts can then be grouped together (or run separately) in virtual containers. A container in this case is a way to isolate a single application (or a part of it) with all its dependencies inside a single unit where the main benefit is scalability.

The web application mentioned in the introduction could also be run in containers, either in parts or as a whole. It could e.g. be divided into three parts, a frontend web interface, a backend server, and a database. These three components could be containerised and run separately, offering possibilities to scale each component individually. Need to handle more requests? Fire up another backend container. Reading from the database is being slow? Deploy another database read replica. When demand decreases, scale back down again.

Containerisation can be seen as an abstraction of the server layer, working to develop applications, not maintaining servers.

WHAT IS SERVERLESS?

A serverless application is an application consisting of loosely coupled microservices. It does not mean that there are no servers, it just means we don't need to care about them. Focus is on the code running in the applications, and not so much on deployment. This approach gives an even more fine-grained control over scaling, with possibilities to scale each component individually. It consists of dozens or even hundreds of functions, where each of these is a tiny little piece with its own policies, roles, API connections, audit trails, etc. This is highly beneficial, and the article will explore this later on, but it also comes at a price in terms of increased complexity. From a security perspective, there are also a lot of new things to worry about. Cloud vendors do their best to help out with baseline security, but there are many pitfalls in terms of configuration and usage.

The two main concepts of serverless are Backend-as-a-Service (BaaS) and Function-as-a-Service (FaaS), both of which can be used separately or in conjunction with each other.

It should also be noted that serverless is not a generic solution that fits every project or use case. Large systems with a fairly consistent load 24/7 will probably be cheaper when deployed to more traditional architectures.

BaaS (Backend-as-a-Service)

BaaS targets web and mobile developers who want a simple and easy way to connect to backend services such as databases, messaging platforms, user management, etc. Given the vast number of mobile apps out there, this is a very convenient way to launch products with extremely low time-to-market. Developers themselves can move from idea to released product without having to worry about servers or deployment.

FaaS (Function-as-a-Service)

Where more sophisticated backend services are needed, FaaS provides the ability to write custom server-side software using small, event-triggered, functions deployed to a fully-managed platform. All deployment, resource allocation, provisioning and scaling is handled by the cloud vendor. This provides a highly customisable modular environment where each component can be individually scaled. Also, there are huge benefits from a cost perspective in that vendors only charge for the time the function actually runs, down to a few hundred milliseconds granularity. If the function is not doing anything, the server is not running, and nothing is charged.

The serverless function

One of the most important components in a serverless architecture is the serverless function. In the Amazon world they are called "Lambdas", and in the Google world they are simply called "Cloud Functions". A serverless function is a small piece of code with a very specific task, such as returning search results from a database. There is a small piece of server hardware that starts up when executing the function, but as soon as

the function has done its job a few hundred milliseconds later, the server is shut down. The server handling all the serverless functions then waits in an idle state for the next request, after which it executes the requested function again.

The serverless function executes in a stateless mode, meaning that information is not persistent between executions. However, this is not always true giving a few interesting security challenges that this article will explore later on.

Benefits

Security

From a security perspective, there are some benefits going serverless. First of all, cloud providers are generally much better than the rest of us in securing and patching OSes and server software. Using smaller microservices also give a very fine-grained Identity Access Management (IAM). Each microservice is doing a very specific task and the permissions can be narrowed down to allow access to only what the particular microservice needs.

Scalability

One of the biggest benefits of serverless is that most of the services auto-scale and auto-provision based on load. There is no need for over-provisioning, which is common in monolithic architectures. It also enables auto-scaling for components that traditionally have been very hard to auto-scale, like databases.

Cost

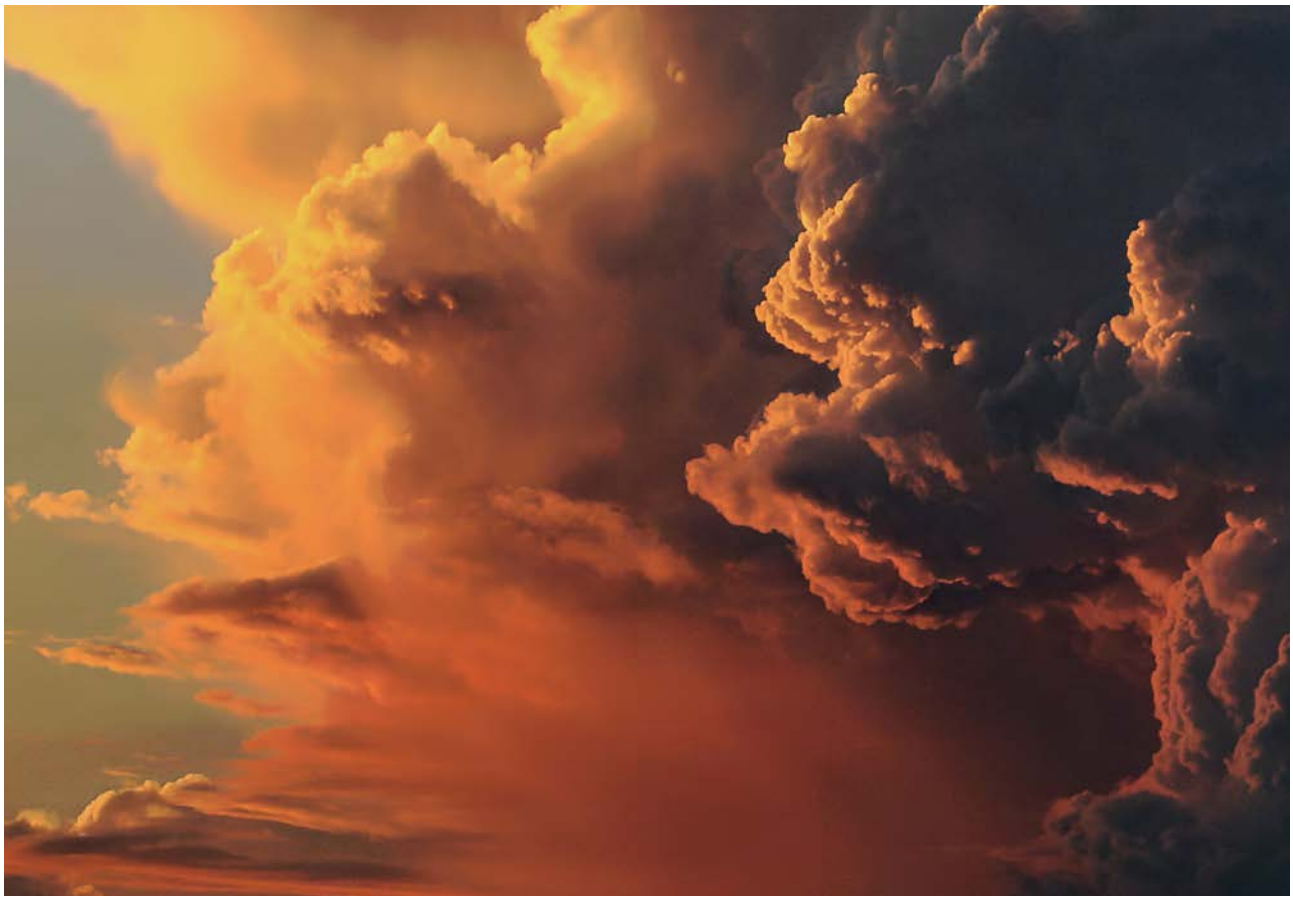
Serverless architecture offers cost based pricing on precise usage, and you only pay for exactly what you use. This can e.g. be measured in the number of read/write requests to a database, the number of milliseconds a function takes to execute, or storage volume.

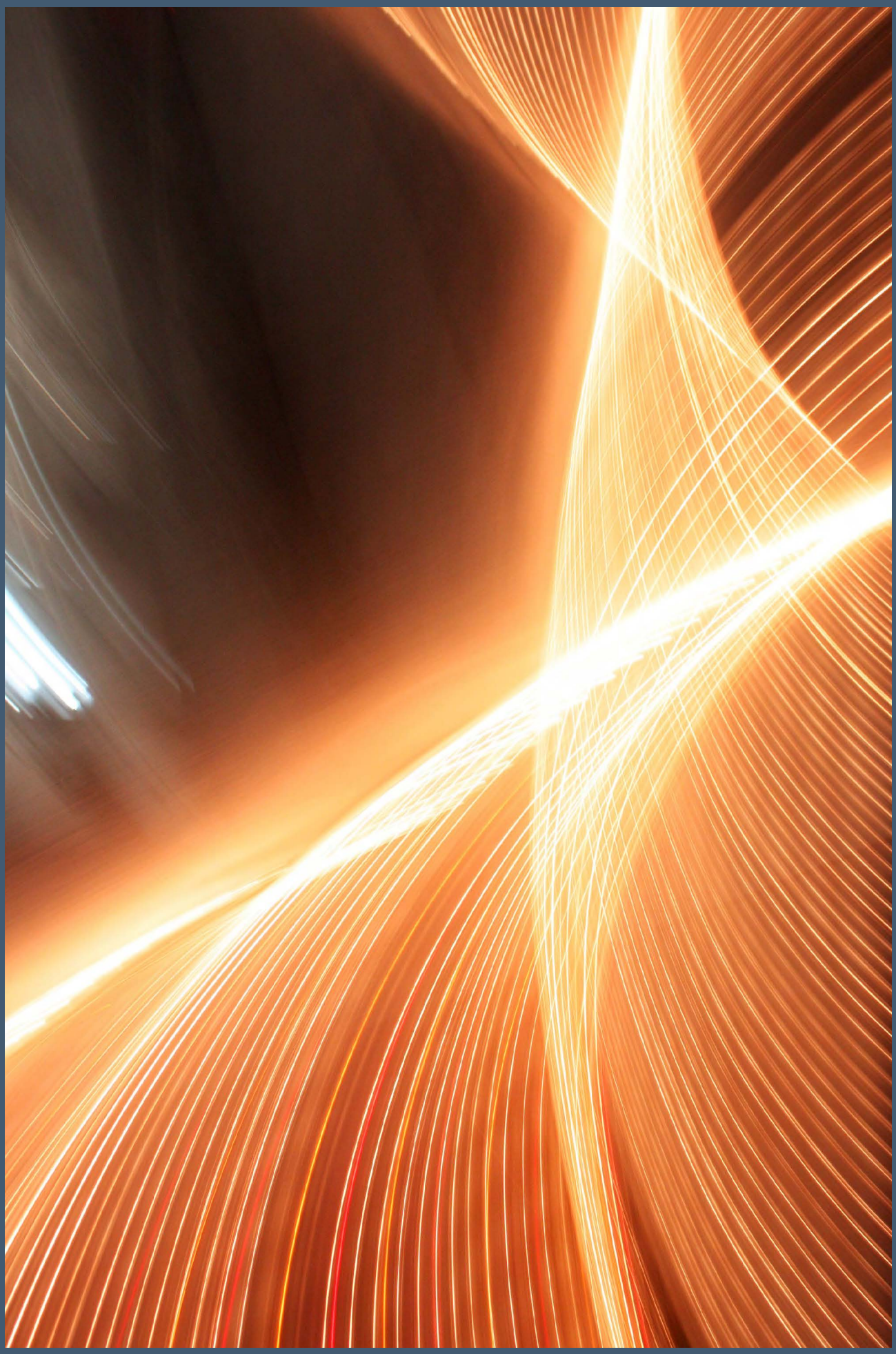
Reliability

A serverless architecture has by design High Availability (HA). For a database, we can assume it's replicated over several instances without us having to worry about it. For a serverless function, we rest assured that if a computation node fails the vendor will instantiate a new one with our code, and re-route the events to the new node. We also assume that if a storage component fails, our data is still safe and that we'll continue to be able to access the data without much interruption. However, this is not the same as Disaster Recovery, and we are still responsible for regular backups, multi-region failover, etc.

Maintenance

The cloud vendor manages the server hosts and server processes. There is no need to keep hardware and software update, since it's all taken care of. ▸





Drawbacks

Security

Persistance

Given the stateless and short-lived nature of serverless functions, one would think that long-term persistent injection attacks are long gone. Attackers however, are creative and there are a number of techniques that can be used to get around this

Traditional vulnerabilities (XSS, SQLi)

Even if applications are running without a managed server, they still execute code. If the code is written in an insecure manner, the application is still vulnerable to traditional application-level vulnerabilities such as Cross-Site Scripting (XSS) and various types of injection vulnerabilities like SQL injection.

Access control

Given the amount of microservices that need individual access control, roles and permissions, the risk of misconfigurations is high. There are a number of ways to mitigate this, where a thorough review of the configuration of the components is key. There are also a number of automatic scripts that can be of value, both as part of a bigger review, or used directly in the DevOps chain when deploying the applications.

Attack surface

A serverless architecture consists of multiple components such as APIs, storage, and message queues that communicates with protocols and complex message structures. Many of these components need to be exposed to the public internet, which increases the attack surface dramatically. Again, since the architecture is still new, the probability for misconfigurations is high.

Traditional security testing (e.g. scanning) is not possible due to the nature of serverless systems, and most automated scanning tools have not adapted to scan serverless architectures. New tools appear more and more often though as serverless gains popularity. The cloud vendors themselves are also constantly evolving, releasing new security features regularly.

Data in transit

With serverless, data is now constantly in transit between various functions. Each time data moves from one place to another, the chances of data being leaked and/or tampered with increase. It's important to make sure that data is secured at all times, regardless if it's at rest or in transit.

Complexity

System complexity

The high number of functions also means that it will be difficult to monitor them. Knowing what to monitor and how will be key in keeping control over a serverless architecture. As the number of functions increase, there is also an increased risk of having unused, vulnerable and/or outdated code in production, which can cause security issues.

Thousands of microservices generate a lot of logs and events. Making sense of all the data can be a challenge, and it might be difficult to know what to look for. Keeping logs and information in a structured manner is even more important in a serverless environment. Also, due to the stateless nature, it might be difficult to know what happened before or after an event.

Lack of perimeter

Serverless architecture changes the way we look at perimeter security since there is no perimeter. All microservices have their own interfaces and protocols. This also raises the question of where to install security controls like firewalls and intrusion detection and prevention systems (IDS/IPS). Traditional security solutions might become irrelevant since customers cannot control and install anything on the endpoint and network levels.

Why isn't serverless super popular?

There are a lot of benefits with a serverless architecture, but the amount of applications running completely in a serverless environment is still quite small. It's important to remember that the change from a monolithic server environment is dramatic. Going completely serverless requires an architectural change of both the applications themselves but also the state of mind of the developers and management. Serverless changes how we design applications, and all components need to be event driven. It is not an easy task to refactor an old application to a completely different architecture.

OVERALL SECURITY DISCUSSION

Lifecycles

It's easy to see that the traditional security approach to a serverless world might assume that attackers can't get a foothold for more than a few minutes at a time given the stateless nature of serverless architecture. One might think that since the functions restart every few seconds or so, even if the attacker gets through the security measures, there is ▸

nothing to worry about since there will not be enough time to gain persistence. Well, in that case one might need to think again. Cloud providers are intentionally vague about how and when they recycle serverless functions, and it's easy to oversee the fact that these functions can live for hours, or maybe even days.

Cold and warm start

In order to increase performance and keeping latency as low as possible, cloud vendors utilise the concept of cold and warm start of functions. The first time a function is executed the virtual machine is instantiated, loaded with the code to execute, and the code starts to run. External libraries used by the function is also loaded which adds up to the total start-up time. This is called a cold start. Due to cost and latency both the user and the provider want to avoid this kind of behaviour and functions are kept "warm" for longer periods of time to make sure the requests are handled as quickly as possible. Within a certain timeframe, consequent requests are handled by a virtual instance that is already running, standing by to serve requests immediately.

This gives great improvement in performance, but unfortunately, it comes with a severe security impact that can be easy to overlook. All of a sudden, our stateless, non-persistent, self-destroying function is now stateful, persistent and might not be destroyed for hours. Plenty of time for an attacker to cause a lot of trouble. This can be achieved in several ways. There are techniques to keep functions warm, and several attacks can be broken down into smaller pieces. For example, an attacker could exfiltrate files from a server one file at a time, or a whole database one record at a time. As said before, attackers are creative by nature, and new attack vectors are invented almost every day.

Example: Ransomware

One of the most common attacks of today is the infamous ransomware. A frightening, red screen with a warning message that all your files have been encrypted, and that you have to pay money to get the decryption key. If an attacker gains access to a serverless file storage, it's not that difficult to leverage this into a full-blown ransomware attack, encrypting one file at a time until the whole file storage is encrypted. Sure, this will need a few thousand function calls, but for an application executing a million calls every second it's not that easy to notice.

Hence, another approach for handling security incidents must be considered, and one possibility is to start focusing on patterns instead of individual calls or events. The patterns should be carefully monitored, and alarms setup in order to get an early warning of what's going on so that it can be addressed without too much delay.

Forensics

Imagine a scenario where an attacker successfully steals sensitive data or encrypts all databases. What do you do next? All servers running the small pieces of code are already terminated and all evidence is gone. It's like asking a forensics expert to secure evidence on a laptop where you have already erased the hard drive and reinstalled the operating system. There is nothing left to be investigated.

There are a few ways to mitigate this. First of all, as we have already discussed, logging is key. Log everything: API calls, CPU and memory usage, processes running, commands that are run by remote shells, everything that might be of importance.

Now comes the next challenge. This approach will generate huge amounts of data, and to get meaningful results out of it, the data needs to be organised in a structured way so it can be analysed. Luckily, there are a few good third-party products that can be used to do exactly this. Some of them even take regular snapshots so that the state of the services can be investigated in detail revealing exactly what happened the seconds before and after the actual incident.

Mitigations and best practices

Serverless security requires a different approach compared to traditional security measures. As a start, the most important actions can be summarised in the following main areas:

Security reviews

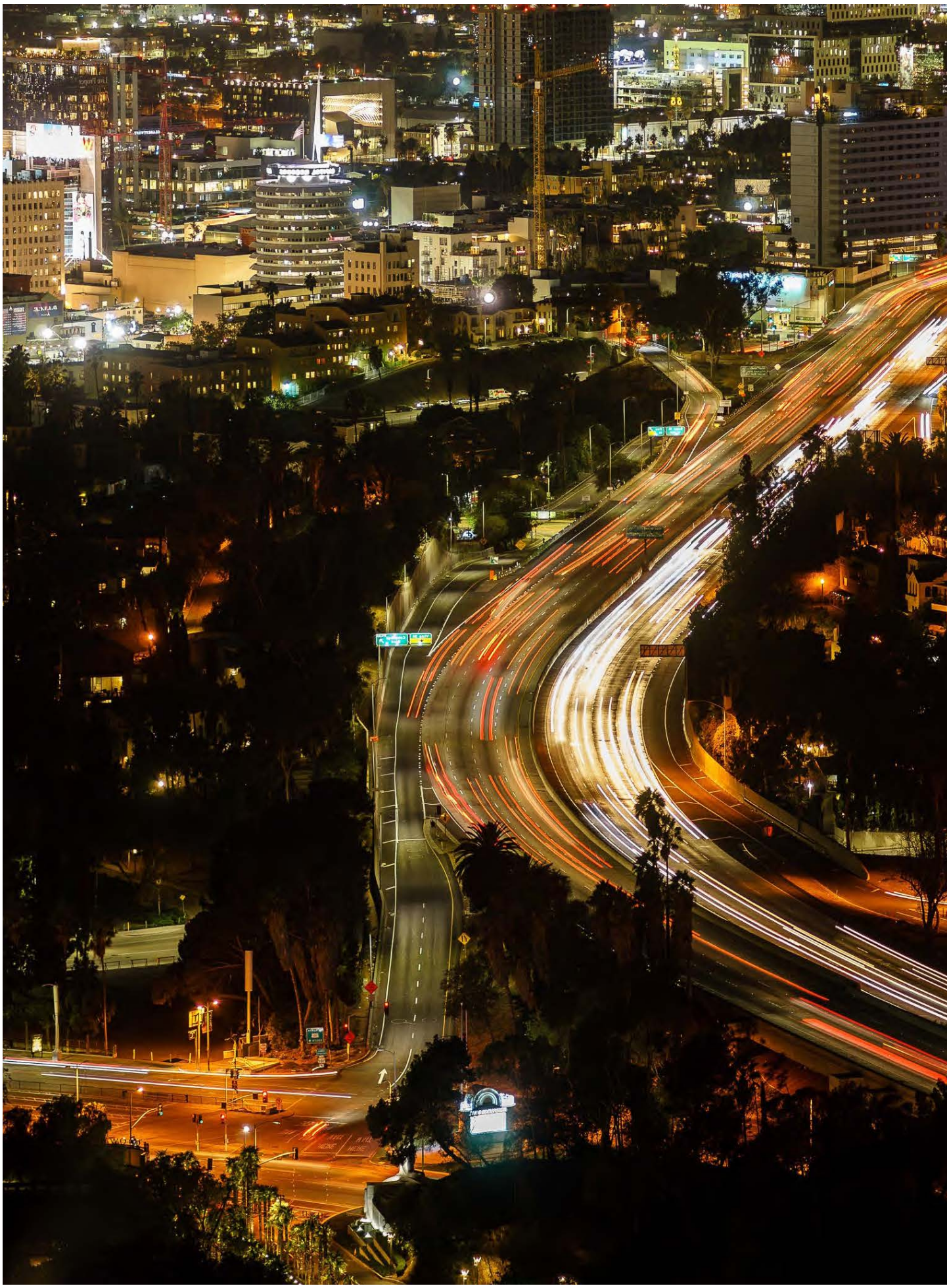
Most serverless applications are, or should definitely be, deployed using automatic scripts. In the Amazon world, this is called "CloudFormation", and the Google equivalent is called "Cloud Deployment Manager". The main concept is that all serverless components such as databases, functions, users, cryptographic keys, etc. are deployed using scripts, usually written in YAML or JSON format. By doing this, one can be sure to deploy exactly the same configuration every time, and there are other benefits as well such as versioning.

From a security point of view there is another huge advantage. Just as you can do a security code review on source code, this also gives you the opportunity to do a security review of the whole infrastructure by just reviewing the scripts describing it. These security reviews should be scheduled regularly,especially when introducing new functionality.

VPC security

The virtual network in the cloud (often called a Virtual Private Cloud, or VPC) is no different from the network in an on-premises environment. There are sub-networks, security groups, firewalls, internet gateways, VPN connections, etc. just as in a physical network. This also means that network security must be considered in a similar fashion. ▸

Serverless security is not that difficult, but it is very different from traditional security



In a serverless environment, classic security structures such as network segregation and firewall rules become even more important since you want to differentiate between the microservices that should be exposed to the public internet and those that should not. You might also want to group services by functionality in order to keep things tidy and to make logging and monitoring easier.

Asset inventory

Create and manage a list of your functions, buckets, tables, APIs, etc. and remember to always keep it up to date! Most cloud providers have built-in tools that can be used to create and maintain asset inventories like this. When you have an overview of what services you have, make sure to get rid of services that are not in use. Old functions and services might be a security risk as an attacker can still call an obsolete function using old keys that they have stolen at a previous point.

Reduce attack surface

Review all your functions and services. What permissions do they have? What other services can they call? Make sure to create a unique role for each function with suitable permission policies. Each function should have permissions according to the principle of least privilege.
Reduce timeouts for functions! Default might be 5 or 10 minutes, which is more than enough for an attacker to do a lot of damage. Most functions only need a few hundred milliseconds to finish its work.

Logging and monitoring

Cloud vendors most often provide thorough and extensive logging out-of-the-box. However, the standard configuration is not always suitable for all companies and configurations, and needs to be carefully reviewed and adapted to fit the specific setup for each organisation. Real-time logs from different systems and serverless functions need to be collected in an organised way for efficient monitoring. These collective logs must obviously also be stored securely to prevent tampering and manipulation.

Third-party software libraries

Code provided from third-party companies that is automatically included from remote servers is a well-known source of vulnerabilities. Make sure to use automated tools in the CI/CD pipeline to help secure external resources. Third-party libraries should always be maintained in a local repository with extra security measures so that potential vulnerabilities are not automatically introduced when a new version of a specific library is released.

Tools

Apart from useful functions from the cloud vendors themselves, there are companies providing software that can really make a difference when it comes to serverless security. Especially useful are the software packages providing an overview of your serverless assets. When there are hundreds or even thousands of microservices it can get difficult to keep track of all of them and all the connections between them. With appropriate software at hand, a graphical overview can be used to track everything that happens in the cloud environment.

Most of these tools also provide logging and forensics capabilities, which is extremely helpful if, or when, an incident occurs. Being able to understand what has happened is obviously key in keeping up to date and improving your security.

GOING SERVERLESS

Serverless security is not that difficult, but it is very different from traditional security. Hopefully this article has explained some important aspects, as well as provided some tools and good practices that can be used and implemented already today.

Finally, it's worth mentioning the OWASP (Open Web Application Security Project) Top 10. The OWASP Top 10 is a list of the most common web application vulnerabilities and is composed by some of the leading researchers and security experts around the world. Due to the different nature of a serverless environment, they recently released a serverless security edition called the OWASP Serverless Top 10. This is a very interesting read for anyone wanting to dig a bit deeper into the subject. ●

GUEST ARTICLE

On Cyber Defense

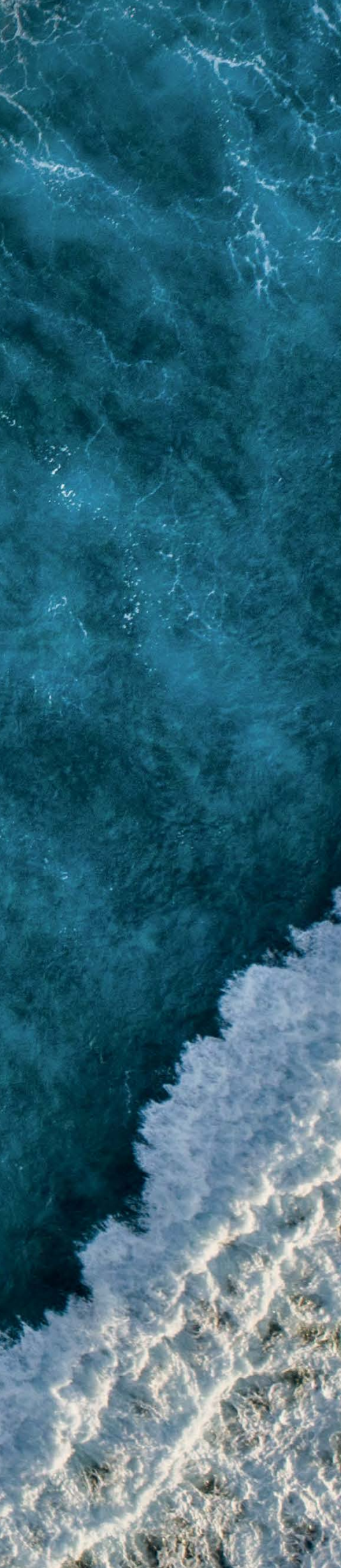
A study in failure

Jeffrey Barto
CISSP

ABOUT THE AUTHOR

Jeff has over 20 years of diverse technology and security experience from start-ups to global financial corporations.

He is an experienced Cyber Security Engineer and Manager, currently focusing on using data mining techniques to reduce false positives and threat validation automation.



In defining cyber security direction, how we implement technology and process while reviewing the threats and risks that impact our environment, the aspect of failure will factor into what we perceive compared to what would actually occur. Taking this concept into cyber security, as cyber practitioners we look at trends across the industry to best align our defenses and use this intelligence to determine what controls should detect and prevent the threat. We then test the controls and determine if the impact of the threat is likely to be caught or not, therefore guiding the direction of your cyber controls towards how that threat works at the given point in time. During this cyclic process, we have multiple areas where mistakes can be made resulting in a failure of the technology or process that can range from being a minor to catastrophic incident.

We rely on technology and the companies creating and improving our use of this technology to meet our demand of mitigating "all" threats perceived valid. We use this technology as the core of our controls adding processes and personnel to both maintain the threat landscape and change when new threats are impacting. When we use technology we are bound by the direction and ability of the technology to meet our challenges in securing the environment. Here, again, we have multiple areas where mistakes can be made resulting in failure. When incidents occur we usually look at the technology involved to blame for the failure to mitigate the threat.

Failed Perception of Root Cause

When we perform a review of an incident in determining a potential "root cause" we usually end up in three main categories: failed technology, failed process, failed action taken or a combination thereof. There is a forth category which is failed perception in contrast to what occurred. This category, in my opinion, contributes to the vast majority of "root causes" for all impacting incidents. Defining this category further, we must determine how mitigation of the threat was implemented into the technology, process, or actions taken compared to the perceived threat attributes and then to the known threat attributes. In turn, the analysis of the incident will direct towards a lack of true understanding, testing, and validation of the threat and the implementation of the mitigation factors. ▸

The cyber technology selected for use within our environment, the personnel hired, the support of management, and the maturity of your cyber security program have bearing on the failure and success in securing the environment.

This, of course, is common knowledge. What is not usually considered is the impact of the cyclic nature of these against the potential for failure. Change occurs quite often in cyber security, whether due to threat vectors, new business technology, personnel, cyber technology, or government guidelines, all factor into the controls established to mitigate threats. Change without validation eventually leads to failure.

Success and failure are a quantitative measure with the ability to gauge incidents and test against the controls holistically. In this case, past incidents can expose how much loss (monetary, reputational, repudiatory) occurred and estimates can be done to determine potential threat impact under the same quantitative measures. Having the ability to understand a threat and the impact against financial loss is key as reputational or repudiatory damage becomes, somewhat qualitative. .

Success and failure are a qualitative measure when using audits, assessments, or frameworks to "rank" the program or controls against peers or certification requirements. For example, when comparisons are made against a framework the view of the implemented control can have attributes that are considered complaint and others that are not depending on the "view" of the auditor or implementer. What is seen here is a "quality" or maturity measure based on the comparison and what the cyber program is designed against. One can be partially successful in comparing to a particular framework then partially fail when attempting to achieve certification status.

Example: Malware infection

If we look at dividing success and failure up in four levels we can label them as follows: success, partial success, partial failure, and failure. If we go further and divide these labels into the *program, control,* and *incident level* we can see that incident level failures impact the control level success and, in turn, these impact the program level success. We will look at a malware infection as an example with the following base criteria:

- The malware infection methods are fully understood.
- Controls associated with mitigating the malware impact are tested and validated.
- Assurance that the control was not modified and revalidated after any change to mitigate the malware is valid.
- All vulnerabilities associated with the malware are fully patched on all systems.
- The likelihood that the malware can impact the organization is high (note this is based on an impact review that the malware would impact the environment if controls fail to block).
- The impact in all three areas is known.

The successful mitigation of the malware infection would now require a test of the sample against the controls implemented and demonstrate all criteria is met. The failed mitigation would, of course, be that the malware infects and completes the infection lifecycle. In between success and failure there are 2 levels that the malware infection can fall into as well. Again, this can be qualitative in measuring the result.

In this well-known area of cyber defense (malware mitigation), we can see the complexity of not only the payload but the multiple areas necessary to fully mitigate a known, analyzed malware infection. We can also see that multiple areas of all 4 levels of success and failure can be assigned to the base criteria from above. What is not seen is the potential of failure from perception of the controls, infection attributes, and program maturity understanding.

Cyber Security is defensive in nature; we defend our data and technology against threats

Achieving Success

So what is failure in relation to Cyber Security Defense? We can take events that do not materialize into incidents and say that our controls were successful in blocking the potential incident, we can measure the maturity of our program with certifications and audits and checkmark compliancy, we can establish automation and continuous testing, on-demand patching, and control validation that shows our controls are well-established to mitigate the current threat landscape, but does this achieve success? We know that all risk cannot be mitigated as there are a lot of factors, complexity, and influence that drives our program.

As I have alluded to throughout this article, technology in itself cannot be the solution alone. To be able to achieve success and strengthen your defenses you need to build and maintain the right expertise among the people working in your team. This requires us to invest in the human capital we have available and understanding that for your people to make the right judgment calls under pressure facing a real threat, they need to have practiced the scenario their facing time and time again.

Cyber Security is defensive in nature; we defend our data and technology against threats. We might incorporate offensive teams or use automation to look for openings in our defenses but chances are the threat actors will find new vulnerabilities and use them first. We, in turn, rely on others to be "the target" and use what is disclosed to strengthen our defenses accordingly. However, rather than passively waiting for relevant discoveries to come your way, you might find it more valuable to actively participate in and share with the security community on a regular basis, and sacrificing time and energy on others to build a mutual trust – then you will find that others become more willing to share with you as well.

GUEST ARTICLE

Modern Crime: Expectations & Challenges

Stig Andersen
PhD Researcher,
Digital Forensic Research Group, NTNU

ABOUT THE AUTHOR

Stig has seven years of experience in law enforcement. He is currently working as a Special Investigator focusing on Digital Policing, alongside his PhD research project on investigation quality and digital forensics.

50 years ago, NASA put a man on the moon. The task was completed using computers that took up whole rooms, and with teams of experts from different fields, all working together to solve a great challenge.

Today, while many of the people from the Apollo program still live, every one of us have more computing power in our pockets, than what one of the largest scientific organisations had at their disposal when they performed one of mankind's greatest achievements.

How can we remain safe and secure in a world that is moving so quickly? asks Marc Goodman, the author of the widely read book on law enforcement and technology *Future Crimes*[1].

Crime adapting to new technology

Crime and uncertainty have been a part of human civilisation since long before we went to the moon. And while we won't see the end of it, it doesn't mean we will ever stop trying. Humans have sought justice and security throughout history. We have built walls to keep away danger, we spy and surveil to keep an eye on threats and valuables, and we track down and punish those who break the rules. So it has been, and so it will remain.

With rapid development in technology comes an equally rapid change in society. The invention of the computer has brought along with it the birth of new industries, new ways of communicating and interacting, and new social challenges. These changes are profound, impacting cultures and communities in ways we haven't even begun to understand. They have also changed the way crimes and threats are manifesting themselves.

New manifestations

For a long time, robbery, for instance, was a violent crime often involving weapons and a fast get-away car. The big heists of today are perpetrated with keyboards, computer code, lies and deceit. Like in the case of "Operation Jackpot", where criminals in one country "robbed" a local branch of an international corporation of almost $60 million USD[2]. While the methods by which the crime was perpetrated were new, the crime remains the same.

Even sexual crimes, perhaps one of the oldest crimes, have completed the transition into cyberspace. There are an increasing number of cases being investigated where rape and other forms of sexual violence are being committed without any form of physical contact between victim and offender. The situation has been described by the Norwegian police as a tsunami of cases[3], and several countries have established branch police offices abroad in order to efficiently investigate cross-border cases. ▸

[1 2 3] *See Reference List at the end of the report*

The NotPetya-story is another example of how our society is subject to changing threats stemming from the digital revolution. Even if we just look at what happened at the surface of this historic event, we notice how a small and seemingly insignificant company like M.E.Doc can become ground zero of what turned into an economic disaster to global giants like Maersk without even being the intended target[4].

In my view, these new manifestations of crime beg the same question:

What do we expect, and who do we expect it from?
Do we expect the police to be able to solve all types of crimes?
And do we expect small companies to be able to prevent advanced cyber incidents leading to disruption in global markets and major financial losses?

Who's going to right this wrong?
If the answer is yes, and it probably should be, then we must expect that these organisations, both private and public, acquire the necessary capabilities, knowledge and skills to meet our expectations. And we must allow them to do so.

The next question should be:

Are we expecting too much? Is it reasonable to expect the police to be able to solve zero-day crimes and for small companies to prevent incidents of global proportions?
In our "instantly global" world, national or local companies like M.E.Doc find themselves operating in the same threat landscape as the global giants to which they provide their services. However, they do not have the same operating budget, international presence or awareness as their international customers. Hence, in my mind it seems unreasonable to expect them to have the same readiness or resources to prevent and respond to global threats.

The situation is not much different for law enforcement and other public service organisations. The knowledge and skillsets required to provide and execute even basic social services now include fields that previously or even currently are considered outside the scope of each service's core subject. The medical profession is faced with the threat of pacemakers and insulin pumps being hacked, and the police and other legal professions have to deal with criminals covering their tracks by hopping from country to country, and thereby jurisdiction to jurisdiction, in seconds.

So where do we start?
As society develops and becomes increasingly interconnected with technology, the requirements for taking on these challenges are not only changing, they are also expanding. I've posed several questions in this article, but unfortunately I don't have the answers for how to make this highly complex situation better. What I do believe, is that in order to understand the challenges we are facing, and to be able to safely and securely apply a skill and provide a service, we need to start by making sure we as a society have a broad

[4] *See Reference List at the end of the report*

I suggest we remain optimistic and remember the words of the legendary Swedish statistician Hans Rosling: "Things can be both bad and better"

understanding – irrespective of trade or craft – and a sufficient level of competency in computer science and informatics.

What constitutes a sufficient level will of course depend on the subject, service and individual. But everyone – even refugees fleeing from disasters and war – carries in their pockets enough computing power to run the entire Apollo program. Such ubiquity of advanced technology calls for different expectation; an expectation of pervasive knowledge about a new basic element in society: the computer.

That, I believe, is at least one fundamental step towards safety and security in a lightning fast world. And while we let the change manifest, I suggest we remain optimistic and remember the words of the legendary Swedish statistician Hans Rosling: *Things can be both bad and better.*[5]

[5] *See Reference List at the end of the report*

REFERENCE LIST

Security Gatekeeping in a DevOps World

1. https://www.oreilly.com/library/view/building-a-modern/9781492044680/ch01.html
2. https://overcast.fm/+NvEIQ62xg
3. https://markeldo.com/Email-update-Technical-literacy-vs-fluency-blockchain-and-OSCP-proctoring/
4. http://blogs.esa.int/mex/2012/08/05/time-delay-between-mars-and-earth/

Word on the Street – European Cybercrime Centre (EC3)

1. https://www.nomoreransom.org/
2. https://www.europol.europa.eu/stopchildabuse

Agile Security Strategy

1. https://sabsa.org/
2. https://www.gartner.com/document/3820265

Semi-Automated Cyber Threat Intelligence (ACT)

1. https://nifi.apache.org/
2. https://attack.mitre.org/
3. https://www.misp-project.org/
4. https://passivedns.mnemonic.no/
5. https://www.virustotal.com/

Modern Crime: Expectations and Challenges

1. Goodman, M., Future Crimes - Inside the digital underground and the battle for our connected world. 2015, London, UK: Penguin Random House UK.

2. Widerøe, R.J. and T. Solberg, Historien om "Operasjon Jackpot" - politi spilte direktør og rundlurte svindlere, in VG. 2017, vg.no: Oslo.

3. Moland, A. and S.T. Mon, Politiet: -En tsunami av overgrepsanmeldelser, in NRK. 2017.

4. Burton, G., Maersk pins $300m cost on NotPetya ransomware, in Computing. 2017.

5. Rosling, H., Factfulness - Ten reasons we're wrong about the world - and why things are better than you think. 2018, London, UK: Specter.

You can also find the references at
www.mnemonic.no/references-2019

For more information about mnemonic,
visit **www.mnemonic.no**

CONTACT

CORPORATE HEADQUARTERS

mnemonic AS
Wergelandsveien 25
0167 Oslo
Norway

+47 2320 4700
contact@mnemonic.no

STAVANGER

mnemonic AS
Solaveien 88
4316 Sandnes
Norway

+47 2320 4700
contact@mnemonic.no

STOCKHOLM

mnemonic AB
Borgarfjordsgatan 6c
SE-164 55 Kista
Sweden

+46 08 444 8990
contact@mnemonic.se

LONDON

mnemonic Cybersecurity
Level 39
One Canada Square,
Canary Wharf
London E14 5AB
United Kingdom

contact@mnemonic.no

CREDITS

Lead Editor Rikke Klüver Voll, mnemonic AS
Art Director Alexandra Stenersen, mnemonic AS
Publication Design Itch Design, Oslo
Cover Design Bjørnar Løvtangen, Make Noise AS
Photo Credits Charlotte Sverdrup Photography (page 6, 8, 13, 18, 19, 47, 53) and Unsplash.com

The views and opinions expressed in this report are those of the authors and do not necessarily reflect the views of their respective employers.