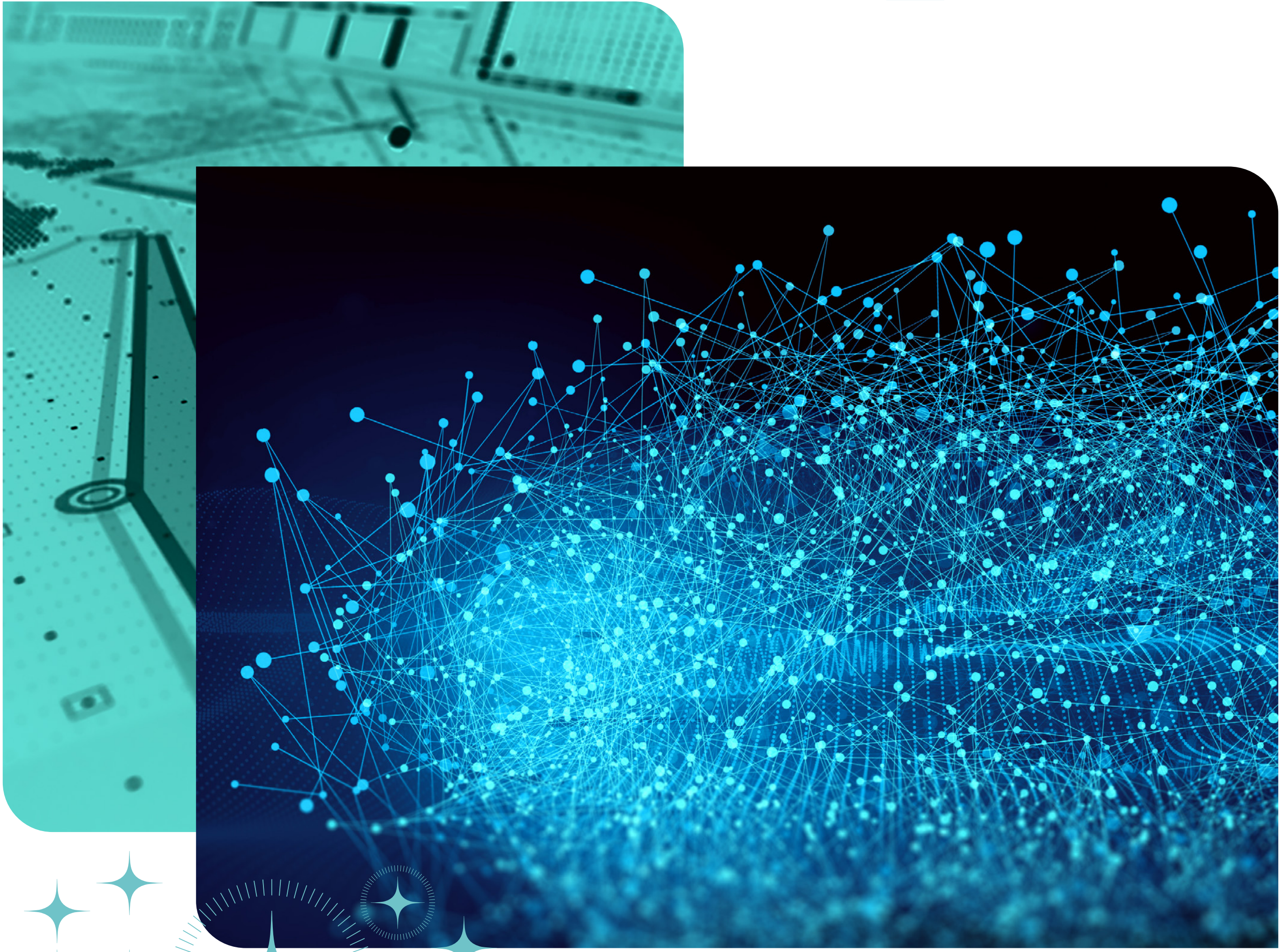
NORTHWAVE
CYBER SECURITY



What Is Next In Cyber Risk Mitigation?

A professional reflection on today's state of cyber resilience and an outlook on how companies can ensure their safe digital journey.

This Northwave publication is a cooperation with:

bytelaw CMS Crawford KRÖLLER BOOM SERVICEPLAN GROUP

Dear Reader,

You are tasked with steering your company in an increasingly hostile digital environment. Gaining the right insights and acting on those have become a crucial part of your daily responsibilities.

We have been accompanying our clients on this journey since 2006. We often first meet them during one of their worst moments: a cyber crisis that paralyses their business and **threatens their existence**.

We have handled hundreds of grievous incident response cases. With each of them, we have not only improved our approach from incident to incident but have also concomitantly developed an international **ecosystem of partners** and a holistic approach to preventing cyber incidents.

I am convinced that these partnerships are the cornerstone of our ability to keep our societies **resilient against digital threats in the future.**

This position paper is the result of the joint efforts of a number of these valued partners and our own experts. Based on our longstanding collaboration in business defence and recovery, it offers you a perspective on what we believe is to come in mitigating cyber risks for businesses around the world.

First and foremost, we want to enable you to successfully avoid disruptions. We are confident that this paper will provide you with concrete guidance to further improve your cyber security and help you understand the elements that will determine your resilience in a moment of crisis.

We wish you a safe digital journey,

Steven Dondorp
Founder & CEO
Northwave Cyber Security

Meeting Of Minds

This paper was created through a series of discussions between seven people, each with considerable **practical experience** in their respective fields in cyber security and cyber incident response.

With their well-versed understanding of what is taking place in the digital underground of the world we live in today, they asked themselves **what is next** in cyber risk mitigation.

These discussions have led to **three key insights**, from which the authors formulated actionable advice for the leadership of companies that want to take their cyber security seriously.

Deven Dobbelaere
Attorney-at-Law
CMS Belgium
Legal & Compliance

Dirk Koch
Attorney-at-Law and Partner
ByteLaw
Crisis Management

Pim Takkenberg
General Manager
Northwave CERT
Incident Response

Paul Handy
Global Head of Cyber
Crawford & Company
Loss Adjustment

Marc de Jong Luneau
VP
Northwave Group
Cyber Security Management

Fabian Prüschenk
CFO
Serviceplan Group
Crisis Communications

Niek Post
CCO
Kröller Boom
Insurance

A Global Outlook On Cyber Risk

The security concerns that come into play when going digital have materialised beyond anyone's wildest predictions. Cybercrime has become an extremely profitable industry, and your digital backyard has transformed into a borderless battle zone for international geopolitical conflicts. How do we see the world that we live in today?

Escalating Threat Landscape

Over the past two decades, the global cybersecurity landscape has seen a significant surge in risk. Since 2001, the number of corporate and institutional cybercrime victims have skyrocketed by 1517%, rising from six to a staggering 97 victims per hour. This exponential growth demonstrates the relentless nature of cybercriminals and their ability to scale the exploitation of vulnerabilities in our digital infrastructure.

The global Covid-19 pandemic exacerbated problems in the cyber security landscape as businesses swiftly transitioned to remote working environments. Cybercriminals exploited the misaligned networks and uncertainty surrounding remote working, leading to a 358% increase in malware attacks in 2020 compared to the previous year. This included many ruthless attacks on healthcare facilities and vaccination infrastructures amidst a global pandemic.

Geopolitics

State-sponsored advanced persistent threat groups (APTs) pose a significant threat to organisations and governments worldwide. This threat is clearly on the rise, with attacks on EU institutions, bodies, and agencies increasing by 30% in 2021. Specific targets continue to be telcos and IT providers, as they are ideal stepping stones for further penetration.

The war in Ukraine has a major impact on the threat landscape, with cybercriminal groups moving into cyberwarfare, leading to a temporary decline in ransomware during the first months of the invasion. Unfortunately, today's numbers are back up and have risen to pre-February 2022 levels in the meantime.

China, Russia, and North Korea are the main adversaries currently threatening Western world economies. With seemingly endless human resources, time, and technology, they are targeting a wide array of data and intellectual property to support their economic growth and the development of their industries.

The techniques employed by APT groups are far more sophisticated and far more challenging to detect then the ransomware gang methods we have become accustomed to. Spear phishing remains a popular method, with almost every APT group utilising this tactic. Additionally, they exploit legitimate administration tools and commercial penetration testing tools to infiltrate networks.

Moreover, we see a marked increase in offline social engineering, and even the recruitment methods that have been standard practice in intelligence communities for decades are now being deployed to support the hacking of companies and government institutions.

Alarming Cost

This all leads to onerous financial consequences. On average, a malware attack will cost a company over $2.5 million, including the time required to resolve the attack. Ransomware attacks, in particular, have become increasingly destructive, with a 57-fold increase in their impact between 2015 and 2021. The impact on individuals is also substantial. Annually, 71.1 million people fall victim to cybercrime, with an average financial loss of $4,476 per person.

The cost of cybercrime is reaching unprecedented levels. Currently estimated at $6 trillion annually, it is projected to reach a staggering $10.5 trillion by 2025. This cost represents 1% of global GDP.

Cyber Risk Insurability

As the threat landscape of cyberspace continues to evolve, the insurability of these risks has become an increasingly critical issue.

Insurers face difficulties in accurately quantifying risks and pricing policies accordingly. On top of that, insurers lack extensive historical data on cyber insurance, which makes it challenging to develop actuarial models and predict future losses accurately.

Furthermore, potential systemic cyber risks pose challenges for insurers in terms of understanding the interdependencies between various industries and accurately assessing the potential impact on multiple insureds simultaneously.

Advances In Cyber Insurance

Insurers are investing significant sums in sophisticated risk modelling techniques that leverage artificial intelligence (AI) and in machine-learning algorithms to enhance risk assessment capabilities. These technologies enable insurers to analyse large volumes of data, identify patterns, and develop more accurate predictive models.

Insurers are increasingly offering tailored cyber insurance policies to meet the unique needs of different industries and organisations. These policies provide coverage for specific cyber risks, such as data breaches, business interruption, and reputational damage, ensuring comprehensive protection.

Many insurers now offer proactive incident response services as part of their cyber insurance policies. These services include 24/7 monitoring, incident response planning, forensic investigation, and public relations support, assisting insured entities in mitigating and recovering from cyber incidents effectively.

Regional Analysis

Governments worldwide are enacting or revising data protection regulations to strengthen privacy rights and enhance cybersecurity. Insurance providers must stay abreast of these regulatory changes to ensure compliance and alignment of coverage with legal requirements. Some jurisdictions have started considering mandatory cyber insurance for certain industries or organisations to ensure a baseline level of protection and incentivise robust cybersecurity practices. Insurers closely monitor these developments and adapt their offerings accordingly.

The global cyber insurance market is segmented into five regions: the Americas, Europe, the Asia-Pacific, and the Middle East & Africa. Due to the presence of several significant insurers in this market and the growing awareness of cyber insurance among SMEs in this region, North America currently dominates the global market for cyber insurance in terms of revenue and market share. Because of its rising levels of liability and cybercrime, the Asia-Pacific will continue to have the greatest compound annual growth rate during the projection period of 2023-2027.

Outlook

Demand for cyber insurance is expected to rise significantly as businesses become increasingly aware of cyber risks and seek financial protection against potential losses. Insurers must adapt their underwriting practices to cater to a broader customer base.

Insurers should invest in educational initiatives to raise awareness about cyber risks, prevention strategies, and the benefits of cyber insurance. Promoting cyber risk education will lead to better risk management practices and informed decision-making by policyholders.

Insurance providers, cybersecurity firms, and other stakeholders will increasingly collaborate to develop comprehensive risk management solutions. By combining their expertise, they can create stronger cyber defence frameworks and improve the insurability of cyber risks.

What Is Next?

Against this global backdrop of developments and based on our experience in insuring and mitigating cyber risks as well as responding in those situations where prevention has failed, what do we see as the most valuable insights that can help companies deal with this situation?

In this paper, we share what we believe are **three key areas** that companies should focus their attention on. They are based on three dominant observations we have made in our practice. In the next three chapters, we will explain why these **insights** are relevant and what concrete **actions** they could inspire to improve your cyber resilience.

Sources:
- https://aag-it.com/the-latest-cyber-crime-statistics/
- https://www.embroker.com/blog/cyber-attack-statistics/
- https://www.griffithsandarmour.com/wp-content/uploads/2021/11/Cost-of-a-Data-Breach-Report-2021.pdf
- https://purplesec.us/resources/cyber-security-statistics/#Cybercrime
- https://purplesec.us/resources/cyber-security-statistics/#APTs

“You Can’t Protect What You Don’t Understand.”

To effectively manage recovery from a disruption caused by a cyber security breach, it is crucial to have a solid overview and understanding of what is going on in the company and its IT and OT environment. That may appear simple to do on the surface. However, our experience in hundreds of incidents has proved exactly the opposite.

The majority of cyber security incidents that we respond to are characterised by serious disruption, with business often even coming to a complete standstill. All data-driven production processes are halted, there is substantial loss of critical data, and digital communications are disabled.

As incident responders, we appear in the victim’s organisation in the midst of this chaos. We need to understand how they operate right off the bat. This is crucial knowledge in bringing them back to business in a sensible way, and this extends far beyond their own digital environments. We need a solid understanding of how their processes function, which of those are critical, which of them are interdependent, and what the alternative routes and processes are. The problem is that most companies lack a comprehensive overview of what they have and how it works.

Understanding

There are tools that help you understand your IT landscape. The most popular is the configuration management database (CMDB). This overview of configuration items allows you to map out the environment. Regular asset discovery by scanning the network offers input. This can be part of vulnerability management.

However, even the most well-maintained CMDB does not provide the complete picture that you need for recovery, as CMDBs do not provide a full overview of how processes work through the systems, how business processes depend on systems outside of the environment, where exactly data is stored, what data is actually there (!), and how data is classified.

Actionable Advice

The best way we know to enhance and maintain understanding is to manage data discovery and classification, to engage in business recovery planning, and to carry out regular exercises and the evaluation thereof. When you make this part of your set of cyber resilience measures (prevent, detect, respond, recover) and manage it as part of **your information security management system**, you enable yourself to respond and recover faster in a cyber crisis.

Most importantly, you want to maintain this crucial information both centrally and outside of your network ('**out of band**'), so it will be accessible during even a complete standstill of your IT and OT.

When looking at adequate protection, we consider APTs to be the new benchmark for cyber security. Implement sophisticated (managed) detection and response and make sure your security partner is IT independent as well as highly knowledgeable. AI-supported detection tools are just a baseline. **You will need good analysts**.

Invest in comprehensive security management and zero-trust security policies as well as in a secure digital ecosystem that safeguards **your supply chains** by protecting data, privacy, and through that, economic stability.

This investment serves a dual purpose. It secures your ability to recover, and it provides good input for the evaluation of risk and effectiveness of mitigating measures (information security management). In addition, this will strongly support compliance with regulations such as **NIS2** and **GDPR**. After all, you can only protect what you know you have.

Out Of Band

We have seen it many times. Along with all the other data, all the resilience planning has been encrypted and is therefore inaccessible as well. And together with all the other systems, the systems for email and voicemail are down too.

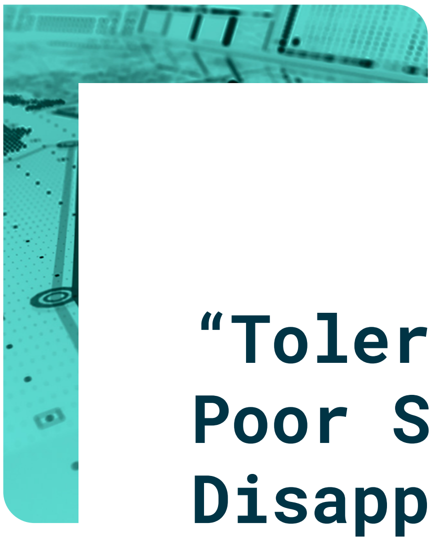
When you want to properly prepare for a crisis, it pays to implement an out of band environment from which you manage your crisis. Such a platform is your global digital war room, providing for:

- **Safe storage and access to incident response, crisis management, and business recovery plans.**
- **Functionalities for all major crisis management processes, such as log keeping, situational reporting, workflow management, coordination, third party management, communication, and documentation.**
- **Exercise support that enables you to practice from this platform and immediately improve your processes and skills from the learnings.**

There are various software vendors that provide these functionalities. We work with:

Merlin

www.merlincrisis.com



“Tolerance For Poor Security Is Disappearing Fast.”

Incidents do not only hurt the victims—a ripple-effect also travels through their supply chains. One incident with a trucking company led to empty shelfs in hundreds of Dutch supermarkets. Dutch consumers had to do without their cheese (a crisis if there ever was one), and producers were left with perishable inventory, storage problems, and financial damage.

Regulators are seeing the increased need to tighten cyber security and data protection. In the European Union, the direction is clear: the EU wants companies to tighten security and better prepare for potential cyber incidents. ENISA (the European Union Agency for Cyber Security) is already setting up technical guidelines on how to secure the processing of personal data. The regulatory pressure that is meant to bolster our economies will be even greater in the **NIS2 directive**. Therefore, companies will have to get clear on their future cyber security strategy.

Wake-Up Call

Similar to the GDPR, the NIS2 directive will specifically demand state-of-the-art cyber security. Today, ‘state-of-the-art’ is still an undefined standard which some companies allow themselves to interpret loosely. We expect those days to soon be over. Owners and **leaders of companies will be held accountable** for their decisions. When it comes to the GDPR, management can already be held accountable for misguided policies or procedures within those companies.

NIS2 is an even louder wake-up call to those who (still) do not have adequate cyber security management in place. They are not only responsible for the wrongful handling of data but also for the delay in controlling the processes of the persons responsible for handling data in a company.

To Fine Or Not To Fine?

The general sentiment around fines for NIS2 non-compliance is still to take measures on what is happening (or, rather, not happening) when it comes to GDPR enforcement. Authorities are seen as somewhat toothless tigers who lack resources. So far, authorities seem to have also been shying away from fining companies, especially when those companies have just been the victim of cyber criminals and are already bleeding.

There is a trend, however, of authorities **increasingly issuing fines**. Markets have been given five years now to make sure they comply with the GDPR. We expect that authorities will be much less patient around NIS2 non-compliance. Note that being fined will also amplify the effects of a cyberattack on your reputation; after all, you are now ‘guilty’.

Supply Chain

We think the key driver in NIS2 adoption will be the pressure it puts on many companies through their supply chains. Not will only the company itself have to comply with many more specific directives with regard to both information security management and measures, but their key supply chain partners will also need to be adherent. This will cause a major (very much intended) trickle-down effect, **bringing the requirements of NIS2 to many more companies than just those that need to comply directly.**

A recent workshop survey among around 50 CISOs and CFOs of midsize and large companies proved that this part of the NIS2 dossier is the major concern for all of them. It is unclear to them how they can get a grip on their suppliers and have their clients want to uphold the requirements. As professionals we have developed answers to these concerns.

Actionable Advice

The previous section has already made clear that getting the right people together to identify risks in individual data processes will lay the foundation for a subsequent successful cyber defence. Furthermore, in the very near future there will be a need to increase compliance management systems in both areas: GDPR and IT security.

NIS2 will demand an integral approach to cyber security management. We expect in general to see contracts change and more prominently feature cyber security and liability clauses concerning any failure to maintain data integrity or continuity. Certainly, cyber insurance providers will adapt to the NIS2 and adjust their policies in accordance with the regulations.

We advise you to resist the temptation to only focus on compliance. Execution of a strategy where security is put first and is centrally managed through a mandated and adequately equipped Security Office will prove the most effective approach in the long term. Our suggested motto for your security operation would be ‘**compliance follows security**’.

“Confident Leadership Determines The Outcome Of A Crisis.”

True story: *The two owners of a large manufacturing company supported their crisis teams during an all-out ransomware incident. Not interfering with the actual work, they served coffee and cake and made sure that the food the teams got was excellent. By remaining warm and calm, they signalled: ‘We have confidence in your ability to save our business.’ For the people who were on the job day and night, this trust from their bosses was a huge boost.*

Rational Reasons

A study conducted by Deloitte in 2019 titled ‘Reputation@Risk’ surveyed executives from various industries and found that 87% of respondents considered reputation to be their most significant strategic risk. The study further emphasised that reputation is the most valuable asset that directly affects an organisation’s bottom line and can account for a substantial percentage of its market capitalisation.

According to a survey by Kaspersky Lab, 32% of consumers stated that they would cease using a company’s services after a data breach. The Ponemon Institute’s 2020 Cost of Cyber Crime study reported that companies experienced an average customer churn rate of 3.9% after a data breach. Four percent might not sound too problematic unless your biggest clients are among the ones leaving you.

It is a fact that companies with robust crisis management strategies and effective communication practices tend to experience more resilient stock performance both during and after a crisis. Their stock prices may still be impacted, but the decline is generally less severe and of a shorter duration compared to companies that mishandle crises.

Emotional Intelligence

Those are the numbers, but what determines good crisis management, and how can you yourself improve in this area? Of course, there are many factors that can be found in textbooks and training programmes. In fact, we can help you develop those capabilities through processes, technology, and regular cyber crisis management exercises.

Yet **your personal leadership qualities** will be the vital lynchpin in guiding your organisation through a crisis. Your role is to inspire confidence and maintain stability. Calm and confident crews will help you effectively navigate uncertainty, make sound decisions, recover from poor ones faster, and emerge stronger from the crisis.

Managing a crisis is a human effort. You will need to understand and manage your own emotions and be empathetic towards those of others. Incidents ask a lot of everyone involved. Long hours, uncertainty about the outcome, and feelings of guilt, incompetence, and failure are all very common*. When people feel safe in your company's environment, they are less prone to making mistakes and more likely to be more resilient in general.

Be aware of the fact that a any crisis can create mental impact on yourself and your people. Northwave has done extensive research into this topic in the context of ransomware incidents. You can find the relating whitepaper through this link. https://northwave-cybersecurity.com/whitepapers-articles/after-the-crisis-comes-the-blow

Crisis Communications

Empathy is equally important when facing the **outside world**. You want to communicate clearly and effectively to provide guidance, updates, and instructions during a crisis. This includes conveying the severity of the situation, outlining the necessary actions, and addressing concerns and questions from all stakeholders, with their interests as a heartfelt driver.

Clear communication helps you to minimise confusion, maintain trust, and keep everyone informed and aligned. **Transparency is crucial** in maintaining trust and credibility, ensuring that stakeholders understand the situation and the organisation's actions. This will include a 'weighing of words' to master the legal implications of the information you provide just as much as the transparency.

Actionalbe Advice

Crisis situations require strong collaboration and teamwork. **Foster a sense of unity**, encourage collaboration, and build trust among team members. Empower and involve your teams in decision-making, leveraging diverse perspectives and expertise to find the best solutions.

Rest assured that shame and blame will instantly destroy the confidence that you so dearly need in a crisis. Once lost, this is most difficult to regain.

The importance of **preparedness** for crises is imminent. Invest in proactive planning and risk assessments and develop crisis management protocols. Promote a culture of transparency and continuous learning, seeking lessons from the last crisis (exercise) to improve capabilities. On a technical level, see also our comments (page 8) on how to create an '**out of band**' cyber resilience environment.

When communicating with stakeholders, we recommend being aware of the literal implications just as much as the messaging 'between the lines'. Your audience will have an impeccable radar for nonsense, and you can lose trust only once.

“But What About AI?”

This year, AI has become an even bigger topic than it already was, with the appearance of a new generation of Large Language Models (LLMs). The topic now dominates any and all conversations that even remotely have to do with technology, including the cyber security domain.

From an attack versus defence perspective, AI developments will increase both attack as well as defence capabilities. The arms race that has been running for years between security research and development and hacker tools, will continue without much actual change, as both side will almost certainly benefit from AI.

When looking into the developments of so-called “Generative AI” models, it will be clear that these developments have the potential to change the way most companies work. So it is wise to actively engage with these technologies. Experiment and investigate. When you do this, keep the following in mind:

Privacy. Don’t put personally identifiable information into the computer systems of organisations with which you don’t have a legal basis to do so. For example, you almost certainly do not have no such agreements with OpenAI for ChatGPT, for instance.

Security. Don’t put information that (when pieced together with other information you share) could tell an observer something about your clients or their security or your company or its confidential information. This concerns company names, IP addresses, hostnames, URLs, usernames, email addresses, technologies used and so on.

Correctness. An LLM has no knowledge of what is correct or not, it just performs next-token prediction on text. This means that it sometimes generates complete rubbish, which is easy to see, but also sometimes faults that are harder to spot. It’s also not able to give source references for the answers it gives, so the burden of verifying before using falls on you. Don’t blindly trust its output but use its output.

Please have a look at our whitepaper on “How to securely use Generative AI in your organisation”. You will find it at: https://northwave-cybersecurity.com/white-paper-policies-and-controls-when-using-ai-applications

Your Responsibility

Our future will be digital, so it is crucial that we are able to fend off the malicious forces that infect and attack it.

To fight back effectively, collaboration between public and private sectors, along with ongoing investments in research and development, will prove crucial to fortifying our defences against all these cyber threats.

Governments will not only increase regulatory pressure, but we also see them mobilising their defensive capabilities, enabling and improving knowledge-sharing between government CERTs, intelligence communities, law enforcement, cyber security firms, companies, and institutions.

However, to a large extent, it will still be every business, every organisation, every citizen for themselves. That places undeniable responsibility on you as a corporate leader, to proactively engage with this topic and establish control.

We hope this paper will enable you to do so, and we would be happy to guide you in that process.

With warm appreciation for your attention,

Deven
Dobbelaere

Niek
Post

Dirk
Koch

Paul
Handy

Fabian
Prüschenk

Pim
Takkenberg

Marc
de Jong Luneau