NRB CYBERSECURITY

CREATING TRUST IN YOUR DIGITAL ORGANISATION

NRB

DARING TO COMMIT

CYBERTHREAT LANDSCAPE

Over the years, cybercrime has grown at such an alarming rate that democratic institutions and economic fabrics have been heavily impacted and have lost the trust of their customers.

With breaches continuously making front page news and new regulations coming into force, effective information security has become one of the most important challenges faced by companies today, and hence a top priority for their CXOs. The increasing number and sophistication of attacks, the growing need to share customer data and intellectual property with third-parties, along with maturing technologies such as cloud computing, mobile and big data, all place enormous demands on companies to develop and implement robust strategies for protecting their business.

Connecting security to business agility has become a must.

> “Cybersecurity is a fundamental protection layer for ensuring social coherence and economic growth”
>
> — ***Michaël Boeckx***, *Chief Security Officer at The NRB Group*

CYBERSECURITY AS ENABLER

Security is all about protecting business goals and assets. Security should be seen as enabling business while reducing risks to acceptable levels and thus allowing business to make use of new technologies for greater commercial advantage. Cybersecurity is a digital and technological enabler of business transformation, industrial modernisation and successful development of artificial intelligence (AI). Adopting AI and Machine Learning will enable the immediate detection of malicious activities and the implementation of effective safety measures.

Preventing threats is no longer sufficient. Cybersecurity must also take into account the fact that threats will be successful. Hence, a holistic approach addressing detection and response capabilities must be adopted. Last but not least, prediction capabilities are crucial in order to be aware of threats before they occur.

At NRB, we help public and private organisations embrace this iterative approach through cybersecurity services, solutions and technologies by implementing the following cybersecurity framework.

NRB MISSION

ENABLE DIGITAL BUSINESS THROUGH SECURITY & ETHICS

INCREASE EFFECTIVENESS IN COMPLIANCE

CREATE TRUTH FOR OUR CLIENTS, CLIENTS OF OUR CLIENTS AND SOCIETY

WHY NRB?

SECURITY IS APPROACHED FROM TWO SIDES TYPICALLY:

LEGAL AND COMPLIANCE:

A view of security linked to legal frameworks and controls.

TECHNOLOGY-FOCUSED:

A portfolio of tools and solutions that are implemented.

A successful cybersecurity practice combines both viewpoints and links them closely together to achieve end-to-end success.

THIS IS THE AMBITION OF THE NRB SECURITY PRACTICE.

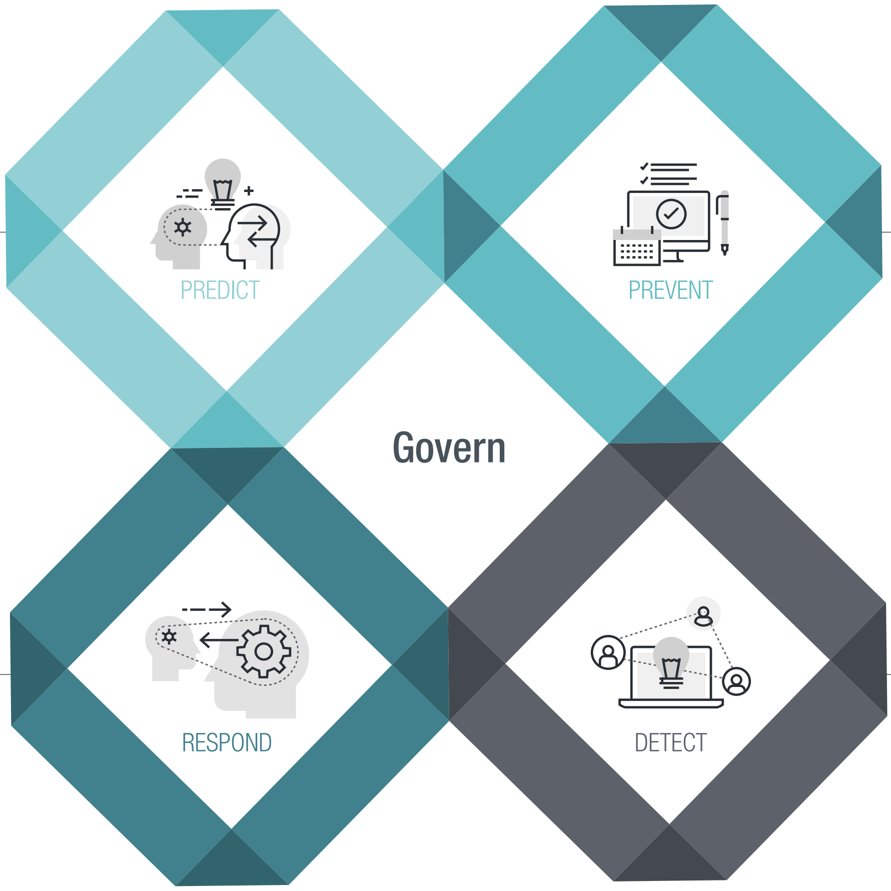
OUR PORTFOLIO

Predict

Governance
Risks
Compliance
GDPR
} As a Service
IT architecture security
Data security governance
Data classification
Data loss prevention
Vulnerability management
Ethical hacking
IT security strategy & roadmap

Prevent

Identity access management
Web access management
Single sign-on
Privileged access management
Firewall governance
Application security
Cloud security
Mobile security
DevSecOps



Respond

Proactive response
Reactive response
Service management

Detect

Security incident & event management
SOC (Security Operations Center)
Threat intelligence
Security incident response
End point protection, detection & response

REGULATORY AND COMPLIANCE

CREATING ROAD TO A SECURE ORGANISATION: ISO 27001

YOUR CHALLENGES

- Understand the profound consequences of changing regulatory paradigms on information systems and organisations
- Meet regulatory requirements in an increasingly tense context where cybersecurity compliance is part of specific regulations
- Assess and address cyber risks which may threaten your business

OUR ENABLERS

- Deliver a comprehensive “as is” and “to be” of a security strategy & policy
- Pilot your cyber risks effectively
- Implement an Information Security Management System (ISO 27001)
- Create a global security awareness culture
- Maximise ROI on IT security spending
- Identify new technologies enabling business while mitigating risks
- Communicate meaningful information security metrics to the board
- Security Awareness Training
  - Train end-users to be a human firewall
  - Assess the human vulnerabilities through the execution of social engineering engagements (phishing campaigns, etc.)

SECURING YOUR DATA: DPO-AS-A-SERVICE

TO ENSURE SECURITY & PRIVACY

YOUR CHALLENGES:

→ Minimise exposure to data breaches and make faster decisions with a clear view of cyber risks across your business ecosystem

→ Prevent attacks on data, theft of intellectual property and business differentiators, sabotage, and information extortion

→ Keep abreast of any change in the law and continually reassess compliance with data privacy and security regulations

OUR ENABLERS:

→ Implement privacy and security by default into existing and upcoming business processes and supporting information systems

→ Implement and maintain compliance with General Data Protection Regulation leveraging processes, people and technology

→ Enable policy-driven implementation of classification, encryption and anonymisation of data

→ Implement a data loss prevention program

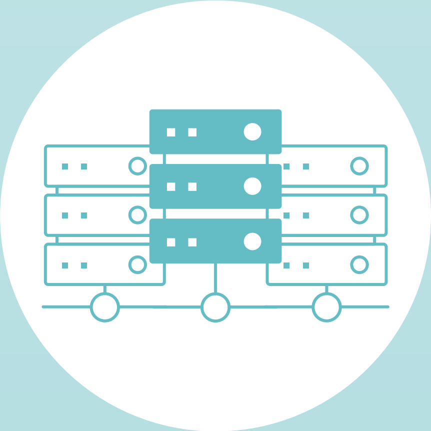
→ Implement and maintain a Business Continuity Plan (ISO22301)

INFRASTRUCTURE AND APPLICATIONS PROTECTION

TO PROTECT KEY ASSETS FROM BEING COMPROMISED

YOUR CHALLENGES:

- Keep pace with continuously growing and more complex corporate networks, data centres and cloud environments
- Protect your digital assets from increasingly sophisticated cyber attacks
- Manage untrusted devices (end points / BYOD) into corporate apps & content
- Maintain compliance with security standards
- Ensure confidentiality, integrity, availability, safety and resilience of the IT ecosystem



OUR ENABLERS:

- Design cyber-resilient architecture
- Protect endpoints (including mobile) against advanced threats
- Optimise firewall operations and security
- Discover vulnerabilities and associated risks
- Verify your cyber resilience through the execution of intrusion testing activities (including Red Team Exercises)
- Identify shadow IT usages
- Secure consumer (BYOD) devices
- Applications Security
    - Discover application vulnerabilities from source code audit
    - Securely integrate cloud environments and applications
    - Enable security of DevOps practice

USER & CUSTOMER IDENTITY MANAGEMENT

SAFEGUARDING YOUR IDENTITY: IAM - CIAM

YOUR CHALLENGES:

- Manage access effectively and securely in complex and heterogeneous environments
- Improve user experience in regard to access management lifecycle
- Obtain a holistic view of rights, permissions and audit risks
- Reduce risk of unauthorised access
- Balance confidentiality and access control, while maintaining flexibility
- Reduce operational costs linked to access management

OUR ENABLERS:

- Define the strategy regarding identity & access management and role-based access management
- Integrate leading IAM solutions
- Enable single sign-on across heterogeneous applications
- Reduce calls to service desk through self-service reset password
- Assign rights to users by non-technical managers with a validation workflow to business
- Build an accurate view of who accesses which applications
- Provide secure access to web applications from the internet
- Enable strong, multi-factor authentication for sensitive access
- Prevent abuse of high privilege users
- Protect customer access and data

ENSURING TRUST ON A DAILY BASIS

A BELGIAN SECURITY OPERATION CENTRE

YOUR CHALLENGES:

- → Detect cyber attacks in a timely manner in order to contain impact
- → Elaborate a formal plan to efficiently manage the increasing number of cyber incidents across different business units within the company
- → Recruit skilled personnel to manage incident responses
- → Monitor critical assets for availability, confidentiality and integrity, in real time
- → Design and roll out a comprehensive security governance plan dedicated to enhancing security, reducing risk and addressing compliance requirements

OUR ENABLERS:

- → 24/7 advanced and proactive monitoring based on defined and dedicated SLAs to protect your critical assets and operations
- → Use cases based on your assets and combined with our experience. We are continuously improving our detection capability with regard to new threats or new kinds of fraud
- → Incident handling, threat management and remediation assistance with first forensic analysis in crisis situations
- → External and internal scans to ensure you are not exposed to new threats

YOUR BENEFITS

- **Pragmatic** implementation of your regulatory and compliance needs (ISO 27001, NIS, GDPR, NIST, etc.)
- Managing your **identity** and **access** as-a-service for you
- An **always-on** security operation centre that secures your digital consumption on a daily basis

USING THESE THREE PILLARS, WE CAN RESTORE TRUST IN YOUR DIGITAL FOOTPRINT

CONTACT

CYBERSECURITY@NRB.BE

www.nrb.be

www.linkedin.com/company/nrb

@daringtocommIT

☎ +32 (0)4 249 72 11

NRB S.A. / nv   Parc Industriel des Hauts-Sarts - 2e Avenue 65 - 4040 Herstal | Boulevard Bischoffsheim, 15 - 1000 Bruxelles / Brussel

NRB

DARING TO COMMIT

bsi. ISO 9001:2015 Quality Management FS 706532

ISO/IEC 27001 Information Security Management IS 706533

Designed at NRB | 02/05/2022