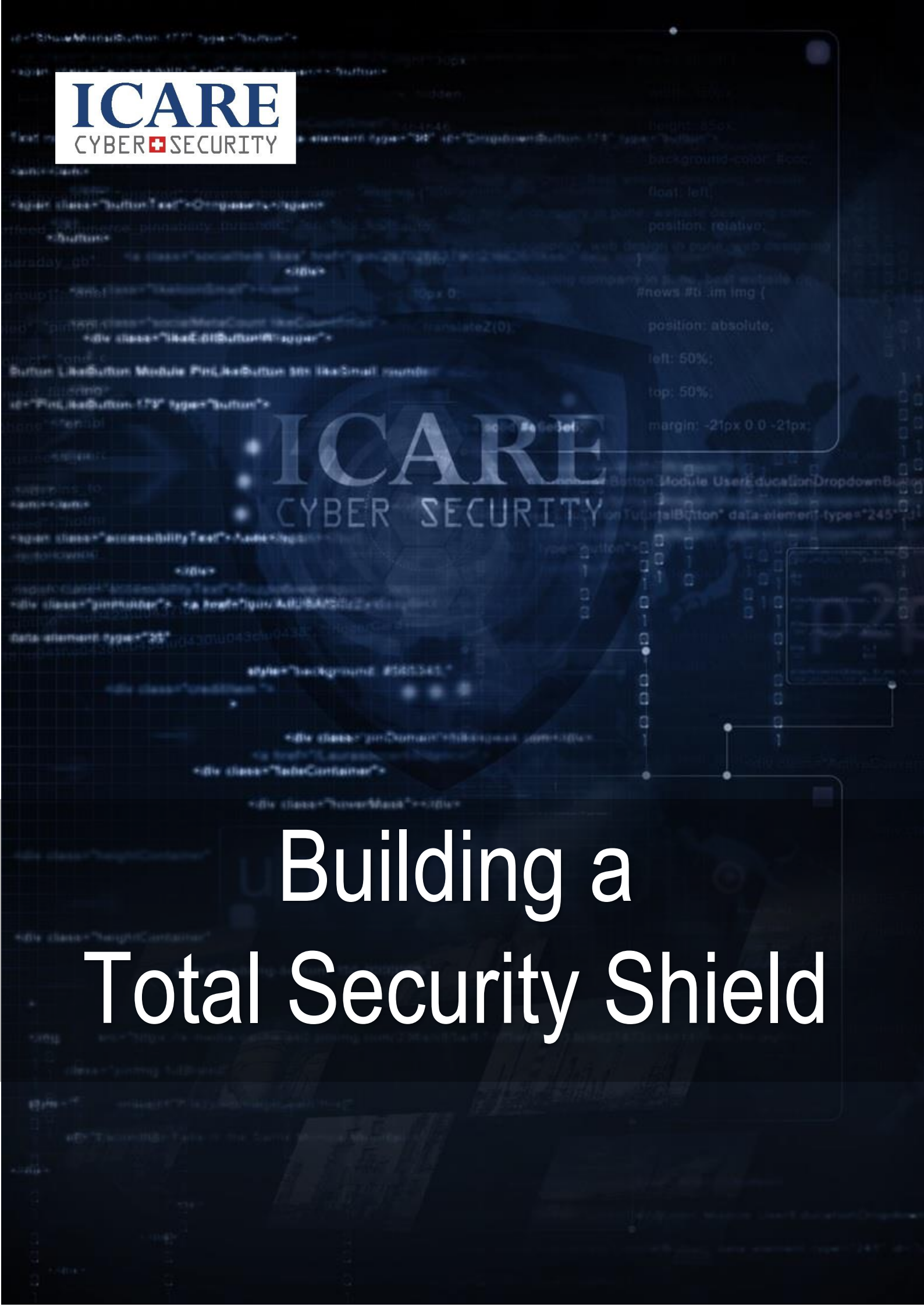

ICARE
CYBER SECURITY
Building a
Total Security Shield

# Building a Total Security Shield

In 2014 **Cybersecurity entered the top 10 Global risk** on the Allianz Risk Barometer. Today it's considered the **3rd largest Risk**. More than **50% of Cyber Attacks** are conducted on Country **critical infrastructure** like Electricity, Water and Oil and Gas **and 75% on Industrial Processes.** Most of those infrastructures were designed for Resilience but never designed with Cyber Security in mind.

Increasingly, traditional Information Technology components are added to the SCADA system (Supervisory Control and Data Acquisition) and PLC (Programmable Logic Controllers), which are increasingly on the Internet, making them prone to Cyber Attacks.

> For example, the **Stuxnet Virus ruined 20% of the Uranium enrichment in 2010** – the Cyber Attack virus was attacking the plants without the operators even realizing what was happening.

Even unsophisticated Cyber Attacks are occurring increasingly on a daily basis as news gets out about the ease of breaches in these SCADA systems.

## *THE SITUATION HAS BECOME SERIOUS*

- Cyber Attacks are causing power outages.
- Massive physical and consequential damages.
- Energy firm are getting increasingly rejected by Insurance Companies.
- Vulnerable and ageing plant control systems, now exposed to the Internet.

## *THERE IS NO EASY SOLUTION*

Upgrading and replacing remote systems is virtually impossible. Firstly, they are scattered over large industrial premises – secondly, their replacement maintenance would require them to be shut down, causing major business interruptions and investment cost.
Furthermore, the solution is not just **Technology** - it is your team's **Training and Behaviour**, and your **Emergency Response Processes** that will determine the degree to which you can protect yourself and mitigate the damage.

## *IS YOUR ORGANISATION PREPARED FOR IT?*

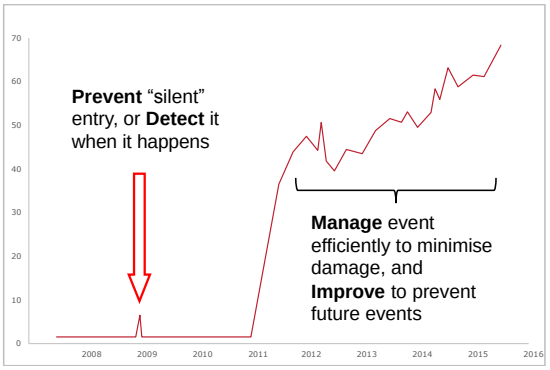
The ICARE Group is a specialist Services Provider to the Power, Oil & Gas, Petrochemicals, Mining and Utilities Sectors – including Advisory, Project Development, Engineering, Construction, EPC, PMC and Procurement Services. We have deep experience of building Utility infrastructures globally.
ICARE Cyber Security is a Division of the ICARE Group that has been created specifically to assist Industrial companies to **Protect** and **Prepare** themselves from Cyber Attacks.
Our state-of-the-art technology, processes and training programmes have been designed around the 4 main pillars of **Prevention, Detection, Management, Improvement** – to protect and prepare our clients to deal with this critical issue.

## *BE READY…*

Our solutions cover personnel training for your internal IT professionals, processes & procedures, and software & hardware solutions – to enable the prevention of an attack, to identify it at the initial stage before damage is done, to manage Cyber Attack events to minimize damage if they occur, and to effectively identify and track the source to improve future defense.

Our solutions focus on 3 core areas:

- **Training:** People training to be able to prevent an attack, identify it at point of entry, and to be able to manage the emergency if the attack is successful
- **Processes & Procedures:** Create and implement a set of Standard Operating Procedures for the organisation to prevent from attacks
- **Systems & Technology:** Data monitoring, control and event management capability to be able to monitor, capture and analyse events in real time as they occur




## *OUR APPROACH*

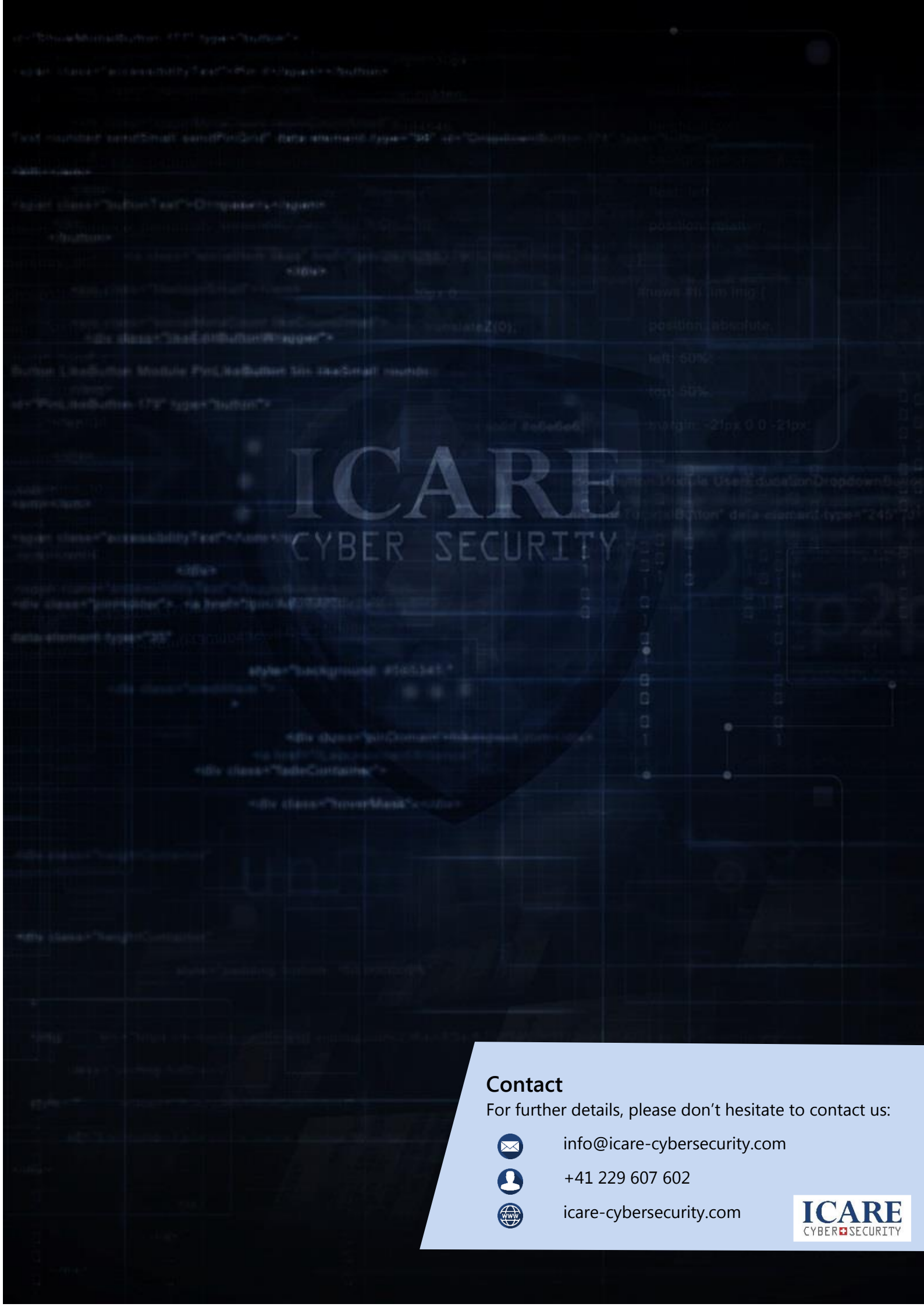
Our approach is to conduct an initial **Gap and Risk Assessment** to define the level of maturity of our customer around **People, Processes & Procedures** and **Systems & Technology**.

Together with the customer, we define an "As Is" and a "To Be" stage and provide a comprehensive solution from implementation through to daily operation.

| Gap & Risk Analysis | Secured Architecture Model | Cyber Security Policy | Security Operation Centre | Response Team | Cyber Training | SCADA Defense |
|---|---|---|---|---|---|---|
| Versatile Environment | ICS Compliance | Implementation Phase | Monitoring | IT Infrastructure | IT Infrastructure | Detection of Attacks |
| Data Bases | Files Sanitations | Define the Opponent | Detection | OT Infrastructure | OT Infrastructure | OSOC for SCADA Systems |
| Remote Access | Segregate Network's | Attack Vectors | Mitigation | Environment Emulators | Risk Assessment | Design & Build SOC |
| Connection between Networks | Secure Data Transfer | Management Commitment | Investigate | Attack Modeling | Risk Monitoring | Secure Architecture |
| Auditing | Secure Remote Connections | Defining Technology Road Map | Reporting | Investigation Technology | Investigation Technology | Consulting |
| Data Leakage | Real Time Protection | Advantage | After Action Analyses | War Games | Forensic | |
| Prevention | | | | | | |

We take you through a transparent, step-by-step approach, to allow you to prepare your organization and protect your critical infrastructure from potentially catastrophic Cyber Attacks.

### PREPARE YOURSELF WITH ACTIVE CYBER COMBAT


## Contact

For further details, please don't hesitate to contact us:

info@icare-cybersecurity.com

+41 229 607 602

icare-cybersecurity.com

ICARE
CYBER SECURITY