CIIP – STRENGTHENING LEGAL, POLICY AND COMPLIANCE FRAMEWORK

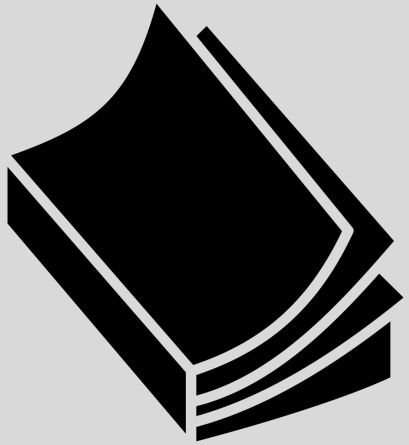
PROF DR MARCO GERCKE

SETTING THE SCENE

CIIP (CRITICAL INFORMATION INFRASTRUCTURE PROTECTION) IS PART OF CIP (CRITICAL INFRASTRUCTURE PROTECTION)

NO UNIQUE DEFINITION (GLOBALLY BOTH RESTRICTIVE AND BROAD DEFINITIONS)

USUALLY: BANKING/FINANCE, TELCOMMUNICATION, ENERGY, TRANSPORT/DISTRIBUTION



ELEMENTS OF A COMPREHENSIVE APPROACH

STRATEGY & LEGISLATION

GOVERNANCE AND REGULATION

DEFINITION AND ASSIGNMENT

PROTECTION

INFORMATION SHARING

CRISIS MANAGEMENT

AGENDA

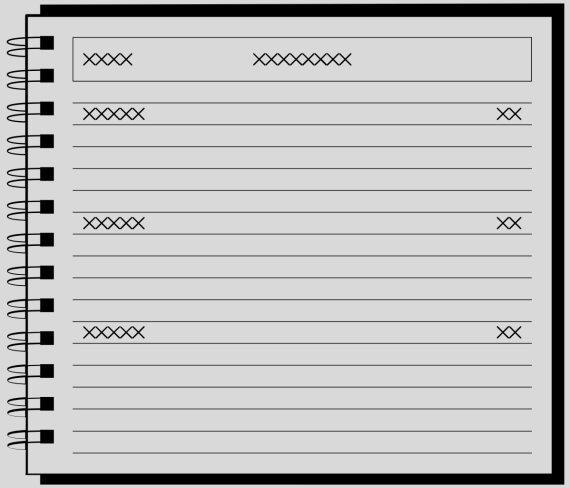
14:00 – 14:10 BRIEF INTRODUCTION

14:10 – 14:50 CIIP INCIDENT SIMULATION

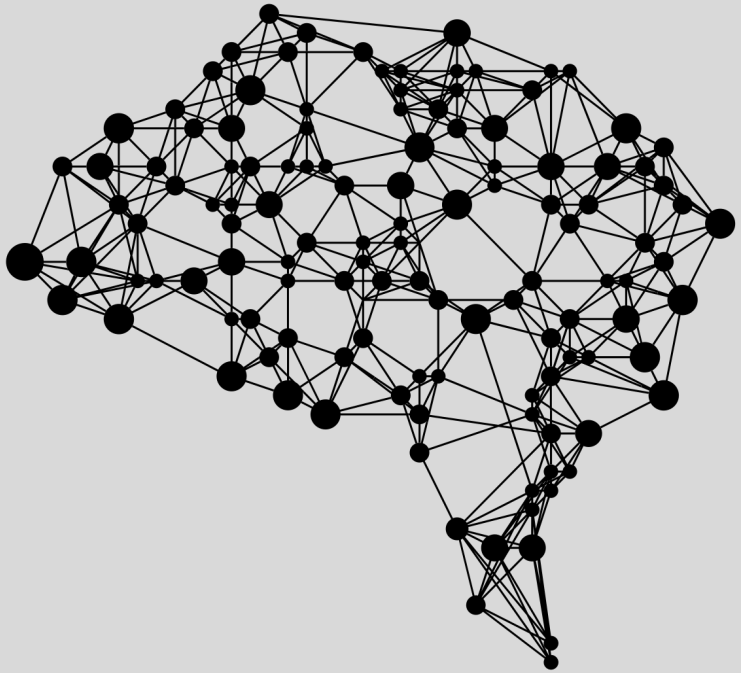
14:50 – 15:00 BREAK

15:00 – 15:30 EXPERIENCE WITH REGARD TO STRATEGY/POLICY, LEGISLATION AND COMPLIANCE FRAMEWORK

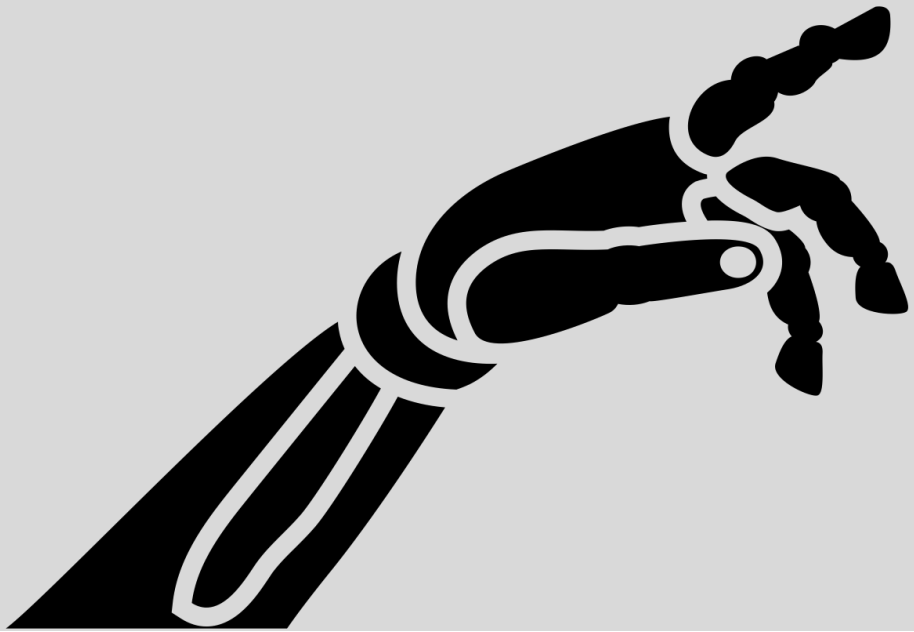
15:30 – 16:00 OPEN DISCUSSION / Q&A



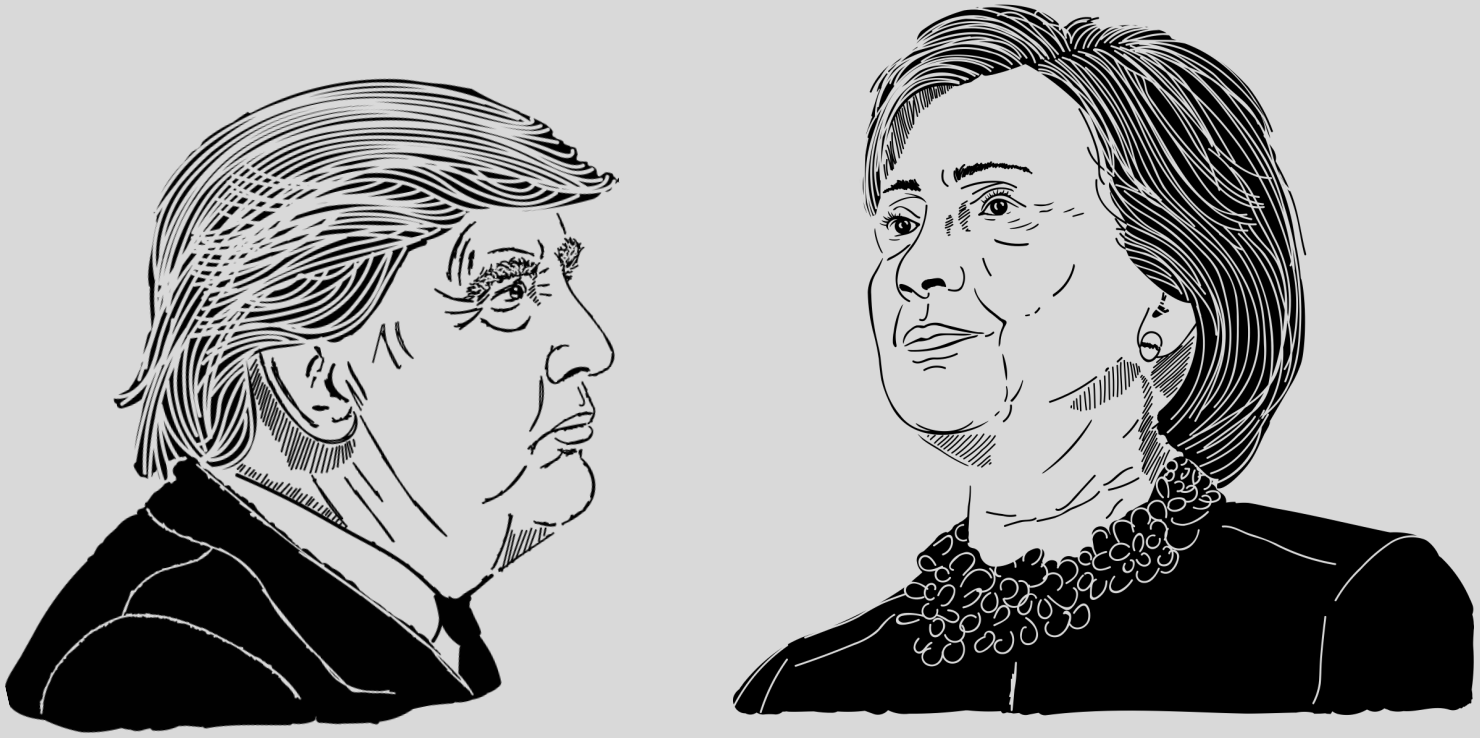
INCREASING DEPENDENCE OF CIIP SECTOR ON ICT



DIGITAL MEGATRENDS ARE FOSTERING THE SITUATION



TOUCHING CORE DEMOCRATIC INSTITUTIONS (EG. ELECTIONS)



LOCAL POWER SUPPLIER

POWER-X IS A LOCAL POWER SUPPLIER WITH ROUGHLY 100.000 CLIENTS. IT IS OPERATING SEVERAL POWER PLANTS AND RECENTLY STARTED TO DEVELOP INTO RENEWABLE ENERGY. THE COMPANY IS ALSO ACTIVELY INVESTING INTO SMART HOMES.

HOW REALISTIC DO YOU BELIEVE ARE ATTACKS AGAINST A COMPANY SUCH AS POWER-X?

1: HIGH RISK

2: MID RISK

3: LOW RISK

IF YOU SEE A RISK – WHAT DO YOU BELIEVE IS THE MAIN REASON?

1: CIIP IS A “RISKY BUSINESS”

2: CIIP IS OFTEN BASED ON OUTDATED TECHNOLOGY

3: THERE IS NO SPECIFIC RISK – IT IS MORE A GENERAL RISK

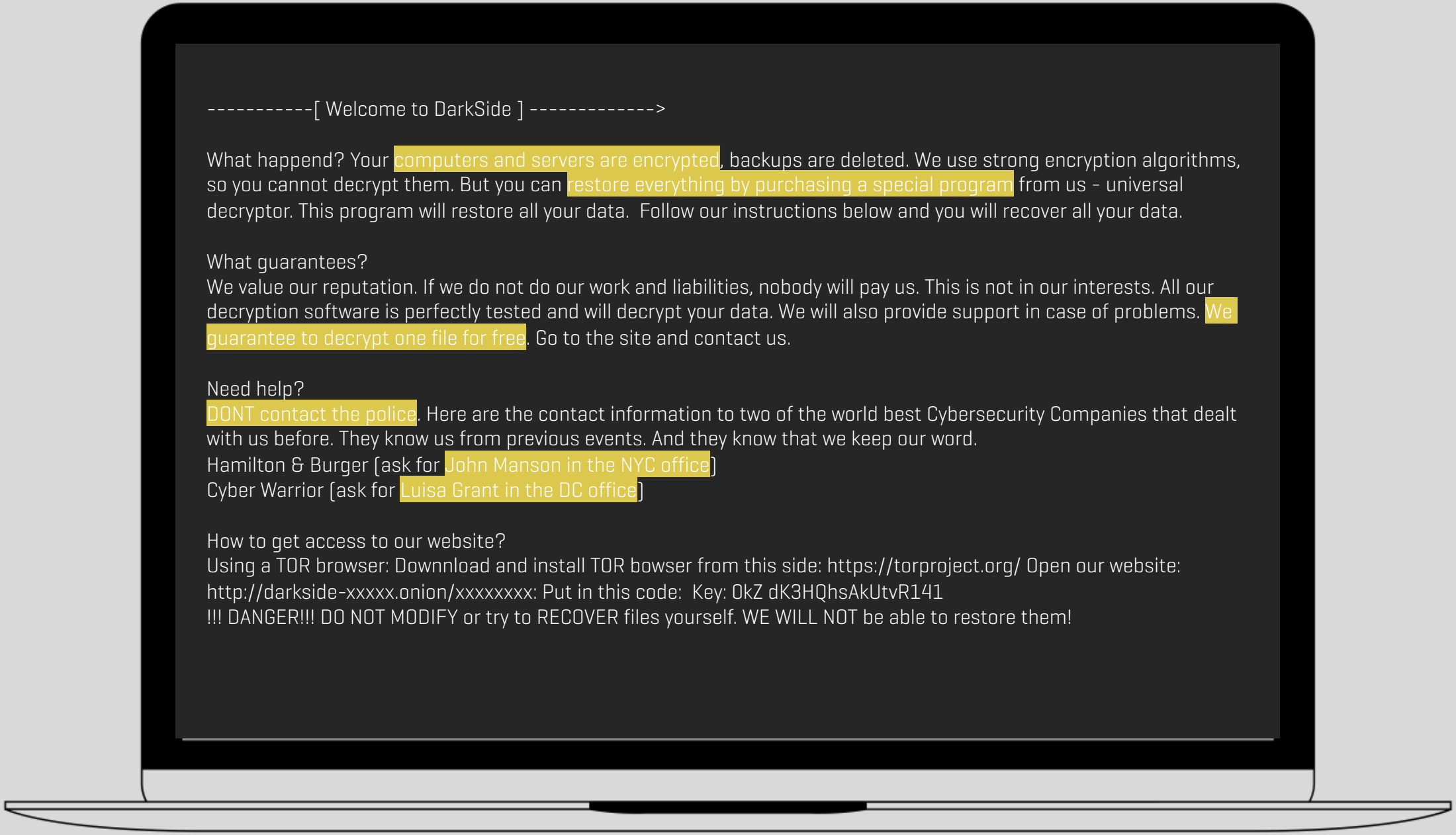
WHAT DO YOU BELIEVE IS THE MOST LIKELY ATTACK?

1: A TARGETED ATTACK AGAINST IT SYSTEMS CONTROLLING ENERGY SUPPLY

2: INSIDER ATTACKS RELATED TO CUSTOMER DATA

3: RANSOMWARE ATTACK


ALL YOUR FILES
ARE ENCRYPTED
FIND README.9d660d45.TXT AND FOLLOW INSTRUCTIONS!


----------[Welcome to DarkSide] ------------>
What happend? Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt them. But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your data. Follow our instructions below and you will recover all your data.
What guarantees?
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests. All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems. We guarantee to decrypt one file for free. Go to the site and contact us.
Need help?
DONT contact the police. Here are the contact information to two of the world best Cybersecurity Companies that dealt with us before. They know us from previous events. And they know that we keep our word.
Hamilton & Burger (ask for John Manson in the NYC office)
Cyber Warrior (ask for Luisa Grant in the DC office)
How to get access to our website?
Using a TOR browser: Downnload and install TOR bowser from this side: https://torproject.org/ Open our website: http://darkside-xxxxx.onion/xxxxxxxx: Put in this code: Key: 0kZ dK3HQhsAkUtvR141
!!! DANGER!!! DO NOT MODIFY or try to RECOVER files yourself. WE WILL NOT be able to restore them!

HOW MUCH WILL THE RAMSOM BE?

1: 10.000 – 20.000 USD

2: 150.000 - 250.000 USD

3: MORE THAN 1.000.000 USD

WHAT COULD BE AN ESTIMATED DAMAGE?

1: 10.000 – 20.000 USD

2: 150.000 - 250.000 USD

3: MORE THAN 1.000.000 USD

WOULD YOU FEEL RELAXED IF THE IT DEPARTMENT INFORMED YOU THAT THEY HAVE A BACKUP AND SYSTEMS ARE UP AN RUNNING IN 24 HOURS?

1: YES, THIS SOUNDS LIKE A SOLUTION TO THE PROBLEM

2: IF THE DAMAGED CAUSED WITHIN 24 HOURS DOWNTIME IS HIGHER THAN THE RANSOM I'D STILL CONSIDER TO PAY

3: NO, I AM NOT RELAXED AS A BACKUP ONLY SOLVES PART OF THE PROBLEM

WOULD YOU CONSIDER NEGOTIATION?

1: I WOULD NEVER NEGOTIATE WITH CRIMINALS

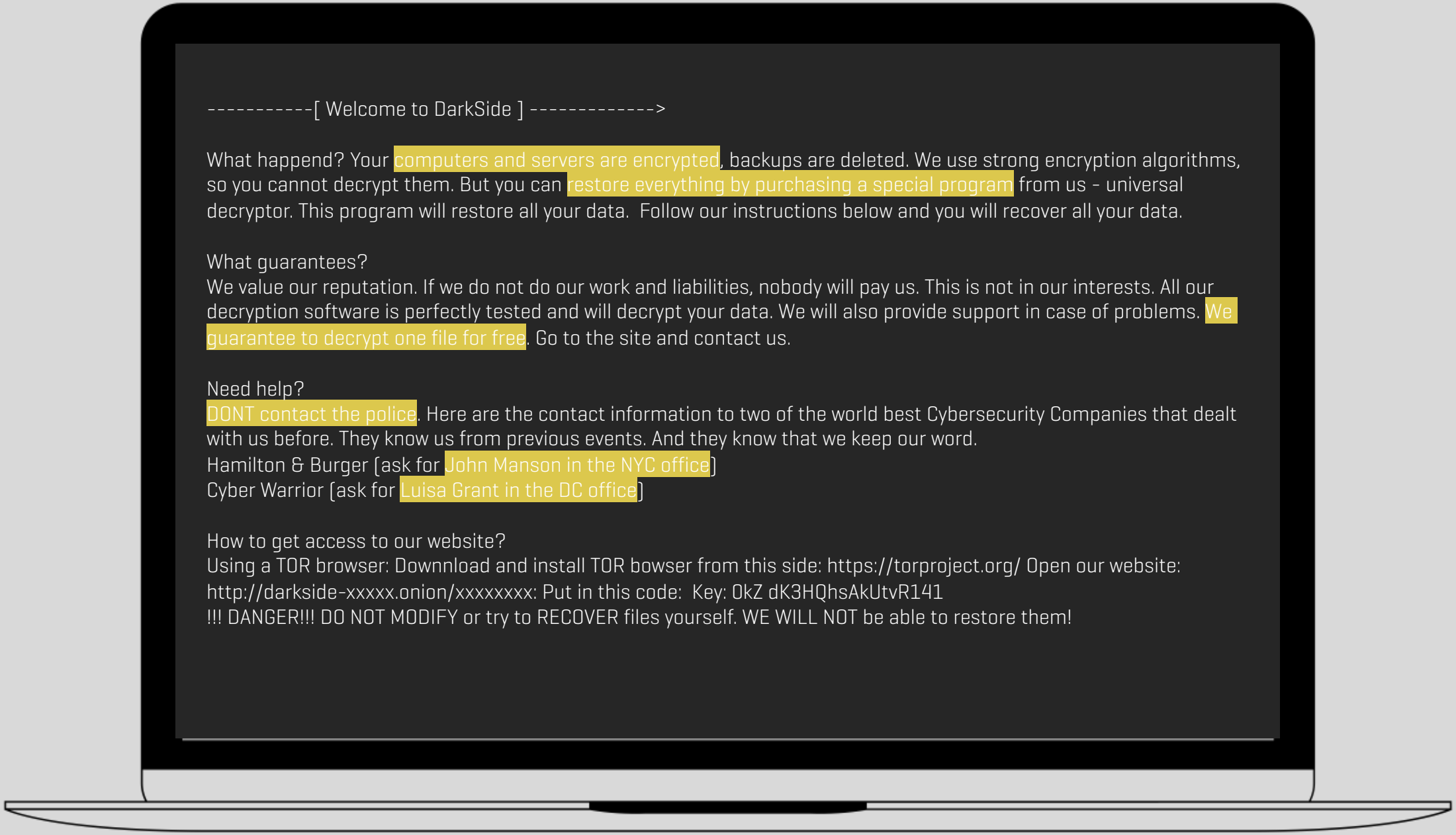
2: I DO NOT THINK CRIMINALS WILL NEGOTIATE WITH ME

3: YES

NATIONAL PIPELINE OPERATOR

C-PIPELINE IS A LARGE PIPELINE OPERATOR, THAT CARRIES UP TO 2 MILLION BARRELS OF FUEL A DAY.


ALL YOUR FILES
ARE ENCRYPTED
FIND README.9d660d45.TXT AND FOLLOW INSTRUCTIONS!


----------[Welcome to DarkSide] ------------>
What happend? Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt them. But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your data. Follow our instructions below and you will recover all your data.
What guarantees?
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests. All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems. We guarantee to decrypt one file for free. Go to the site and contact us.
Need help?
DONT contact the police. Here are the contact information to two of the world best Cybersecurity Companies that dealt with us before. They know us from previous events. And they know that we keep our word.
Hamilton & Burger (ask for John Manson in the NYC office)
Cyber Warrior (ask for Luisa Grant in the DC office)
How to get access to our website?
Using a TOR browser: Downnload and install TOR bowser from this side: https://torproject.org/ Open our website: http://darkside-xxxxx.onion/xxxxxxxx: Put in this code: Key: 0kZ dK3HQhsAkUtvR141
!!! DANGER!!! DO NOT MODIFY or try to RECOVER files yourself. WE WILL NOT be able to restore them!

HOW MUCH WILL THE RAMSOM BE?

1: 10.000 – 20.000 USD

2: 150.000 - 250.000 USD

3: MORE THAN 1.000.000 USD

WHAT COULD BE AN ESTIMATED DAMAGE?

1: 10.000 – 20.000 USD

2: 150.000 - 250.000 USD

3: MORE THAN 1.000.000 USD

LEGAL, POLICY AND COMPLIANCE

ELEMENTS OF A COMPREHENSIVE APPROACH

STRATEGY & LEGISLATION

GOVERNANCE AND REGULATION

DEFINITION AND ASSIGNMENT

PROTECTION

INFORMATION SHARING

CRISIS MANAGEMENT

STRATEGY/POLICY AS A STARTING POINT

USUALLY A CYBERSECURITY STRATEGY CAN BE A GOOD STARTING POINT

SUCH A STRATEGY COULD INCLUDE ELEMENTS RELATED TO CIIP

ALTERNATIVELY A DEDICATED CIIP STRATEGY COULD BE DEVELOPED AND IMPLEMENTED

STRATEGY

STRATEGY/POLICY AS A STARTING POINT

OPEN STAKEHOLDER
CONSULTATIONS CAN HELP
DURING THE PROCESS

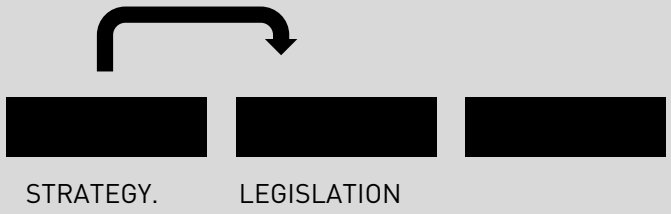
DON'T "REINVENT THE WHEEL"
BUT ALSO DO DON'T SIMPLY
"COPY-PASTE"

BE MINDFUL WHEN CREATING
NEW INSTITUTIONAL CAPACITIES

LEGISLATION

LEGISLATION CAN PLAY A ROLE IN A COMPREHENSIVE APPROACH TO CIIP – BUILDING UPON THE STRATEGY/POLICY

EXAMPLES: PROVIDE DEFINITIONS, DEFINE OR REQUIRE MINIMUM PROTECTION, IMPLEMENT NOTIFICATION REQUIREMENTS, IMPLEMENT MANDATORY AUDITS

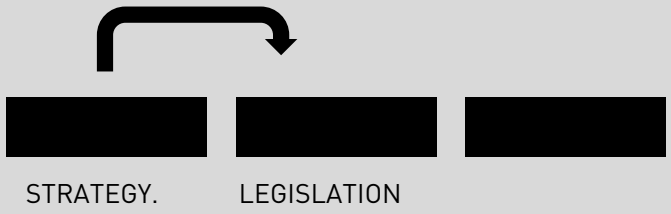


LEGISLATION

STARTING WITH AN ASSESSMENT OF EXISTING LEGISLATION CAN BE A GOOD STARTING POINT

A COMPARATIVE ANALYSIS WITH BENCHMARKS CAN PROVIDE AN OVERVIEW ABOUT GAPS

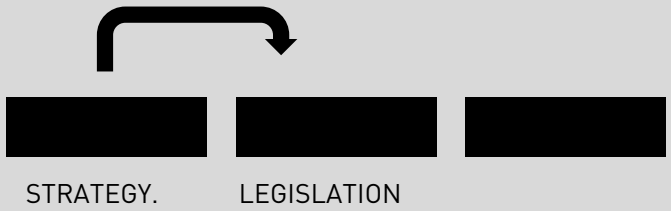
FOLLOWING REGIONAL OR INTERNATIONAL STANDARDS CAN HELP TO ENSURE COMPATIBILITY IN INTERNATIONAL COOPERATION



LEGISLATION

CHANGES IN TECHNOLOGY MAY REQUIRE UPDATES – BE MINDFUL THAT AMENDING LEGISLATION CAN BE A TIME-CONSUMING PROCESS

USING INSTRUMENTS THAT CAN MORE EASILY BE UPDATED CAN HELP

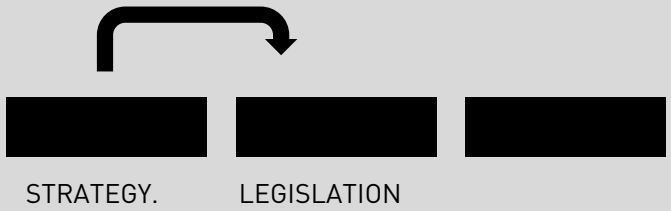


LEGISLATION

STANDALONE VS. INTEGRATION

BOTH APPROACHES OFFER ADVANTAGES AND DISADVANTAGES

BE MINDFUL ABOUT EXISTING STRUCTURES AND NATIONAL LEGAL DRAFTING TRADITIONS



ENFORCEMENT/COMPLIANCE

ESPECIALLY WHEN IT COMES TO CORE ELEMENTS OF CIIP ENFORCEMENT MECHANISMS CAN BE CRUITIAL

EDUCATION AND AWARENESS RAISING COULD BE THE FIRST STEP

DIFFERENT INSTRUMENTS (CIVIL/CRIMINAL/ADMINISTRATIVE)