Critical Infrastructure Security & Resilience

Sokratis K. Katsikas
Critical Infrastructure Security & Resilience Group
Center for Cyber & Information Security
Dept. of Information Security and Communication Technology
sokratis.katsikas@ntnu.no
• Largest University in Norway, 39000 students, approximately 400 PhD dissertations per year
• 4 Nobel laureates
• 120 research labs, more than 90 spinoffs
• 14 faculties and 70 departments and divisions
• FTE: 6700, of which 4053 are in teaching, research and outreach positions (39% female).
Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK)

- 80 ansatte i Gjøvik og Trondheim
- Forskningsgrupper og -laboratorier innen avhengighet og ytelse, biometri, cyberforsvar, forensics, intelligente transportsystemer, internet of things, informasjonssikkerhetsledelse, kritisk infrastruktur, kryptografi, skadevare, e-helse og velferd
- 1 bachelor, 2 master, 1 siv.ing og 2 PhD-utdanninger
- Forskningsprosjekter: EU H2020, EU FP7, EU Cost, EDA, IARPA Odin Thor, NFR FME, NFR IKT+, NFR ENERGIX, NFR BIA, NFR Forskerskole, NFR NæringsPhD, RFF
  Omfang ca 40 MNOK i 2017 (45% av budsjettet)
- Vertsinstitutt for NTNUs Center for Cyber and Information Security
Current research projects

- Positive City ExChange” (CityXChange) – H2020
- Cyber Security Network of Competence Centres for Europe (CyberSec4Europe) – H2020
- Future tamper-proof Demand rEsponse framework through seLf-configured, self-opTimized and collAborative virtual distributed energy nodes (DELTA) – H2020
- Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control (GHOST) – H2020
- Innovation and Excellence in Cyber-security teaching in Higher Education (SecTech) – Erasmus
- Cyber-Physical Security in Energy Infrastructure of Smart Cities (CPSEC) – NFR IKTPluss
- Cybersecurity Platform for Assessment and Training for Critical Infrastructures Legacy to Digital Twin (CybWin) – IKTPluss
- Re-linking the weak link (RELINK) - IKTPluss
- Cyber Power Praxis: a study of ways to improve understanding and governance in the Cyber Domain – NTNU
- Security of the Cyber-Enabled Ship – KD
- Communications and cyber security for Digital transformation project on autonomous passenger ferries (Autoferry) – NTNU
- Cybersecurity, Safety, and Resilience of Smart cities – NTNU
- Artificial Intelligence driven Cybersecurity trustworthy platform in connected medical devices environment (ARMOR) – NTNU
Agenda

- Definitions and taxonomy of critical infrastructure
- National cyber security strategies
- Critical infrastructure security incidents
- Threats
- Vulnerabilities
- The NIST Framework for Improving Critical Infrastructure Cybersecurity
- From security to resilience
Critical Infrastructure - EU

- Critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

COUNCIL DIRECTIVE 2008/114/EC
of 8 December 2008
on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
Critical Infrastructure Sectors

- Information & Communications Technology
- Finance
- Manufacturing
- Food
- Health
- Energy & Utilities
- Water
- Transportation
- Safety
- Government
### CI sectors in EU MS

<table>
<thead>
<tr>
<th>SECTORS</th>
<th>ENERGY</th>
<th>ICT</th>
<th>WATER</th>
<th>FOOD</th>
<th>HEALTH</th>
<th>FINANCIAL</th>
<th>PUBLIC &amp; LEGAL ORDER</th>
<th>CIVIL ADMIN.</th>
<th>TRANSPORT</th>
<th>CHEMICAL &amp; NUCLEAR INDUSTRY</th>
<th>SPACE &amp; RESEARCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CZ</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DK</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>EE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FI</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FR</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HU</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ES</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CH</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Table 1 – Critical Sectors per Country. Adapted from: ENISA, Methodologies for the Identification of Critical Information Infrastructure Assets and Services 2014. p. 5-6*
Agenda

- Definitions and taxonomy of critical infrastructure
- National cyber security strategies
- Critical infrastructure security incidents
- Threats
- Vulnerabilities
- The NIST Framework for Improving Critical Infrastructure Cybersecurity
- From security to resilience
Cyber space

- Lacking a clear definition, a vague consensus seems to define cyber space as the physical, logical, and organizational (social) interconnections arising from interconnecting information systems, also with physical systems.

- It seems fitting that the term was coined by the Science Fiction author William Gibson in a short story (*Burning Chrome*, 1982):
  - *All I knew about the word cyberspace when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.* (W. Gibson, 2000)
Cyber security

- **EU**: Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. Source: CCDCOE

- **Norway**: Protection of data and systems connected to the Internet. Source: [Cyber Strategy for Norway (2012)](https://cyberstrategyfornorway.com/

- **US**: Several – see [https://ccdcoe.org/cyber-definitions.html](https://ccdcoe.org/cyber-definitions.html)
Cyber vs information security (1)

- Information security is about the protection of information, regardless of whether it is stored digitally or not.
- ICT security is about the protection of information and communications technologies – i.e. hardware and software.
- IT security is the protection of information technologies. In practice there is no difference in ICT security and IT security.
- Data security is about securing data.
- Cyber security is about securing things that are vulnerable through ICT.

https://ccis.no/cyber-security-versus-information-security/

Cyber vs information security (2)

- Both concepts aim to attain and maintain the security properties of confidentiality, integrity and availability.
- However:
  - whilst information security started when most systems were standalone and rarely traversed jurisdictions, cybersecurity works on global threats under legal uncertainty. Thus, laws created for information security are woefully inadequate in the Internet era.
  - cybersecurity has to contend with an Internet architecture that makes it virtually impossible to attribute an attack to an actor.
  - due to its origins in the military and diplomatic services, information security typically focuses on confidentiality. Whilst WikiLeaks underlined the import of confidentiality, cybersecurity focuses more on integrity and availability.
- Thus, cybersecurity is information security with jurisdictional uncertainty and attribution issues.

Cybersecurity is a global challenge

- In contrast to land, air, sea and space, cyberspace poses the following unique difficulties.
  - Due to the global reach of ubiquitous networks, threat actors can launch distressing attacks far from victims and often in jurisdictions with weak laws and/or no enforcement.
  - Fast connection speeds give victims little time to defend against attacks. Thus, at best, States and organizations only know about an attack when it is in process. At worst, victims do not discover the compromise of their critical systems.
  - Whereas States pursue national interests through a rules-based international system, cyberspace does not have accepted norms and principles of proportionality.
National cybersecurity strategies

- Enhancing cybersecurity and protecting critical information infrastructures is essential to each nation's security and economic well-being.
- At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and civil society. The formulation and implementation of a national framework for cybersecurity requires a comprehensive approach. This framework often receives a label of a National Cybersecurity Strategy (NCS).

The need for a national strategy

• Treats Cyberspace as a strategic domain
  – Strategies help mitigate the impact of cyber attacks

• Basis for a National Programme
  – The strategy improves security as it provides all stakeholders awareness of relevant risks, preventive measures and effective responses.

• Strategy Builds Capacity
  – A strategy could yield benefits beyond security
Elements of a holistic, multi-stakeholder and strategy-led cyber security programme

• Top Government Cybersecurity Accountability
• National Cybersecurity Coordinator
• National Cybersecurity Focal Point
• Legal Measures
• National Cybersecurity Framework
• Computer Incident Response Team (CIRT)
• Cybersecurity Awareness and Education
• Public-Private Sector Cybersecurity partnership
• Cybersecurity Skills and Training Programme
• International Cooperation
Cybersecurity stakeholders

- Executive Branch of Government
- Legislative Branch of Government
- Critical Infrastructure Owners and Operators
- The Judiciary
- Law Enforcement
- Intelligence Community
- Vendors
- Academia
- International Partners
- Citizens
National cybersecurity strategy model

EU cybersecurity strategy

• Europe’s original strategy for cyber security was launched in 2013. (https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf)

• In 2016, the European Parliament and the Council reached an agreement on the Commission’s proposed measures for the security of network and information systems (the NIS Directive) and on the data protection reform.

• In September 2017, the European Commission reviewed the EU Cybersecurity Strategy and the mandate of the European Union Agency for Network and Information Security (ENISA), to align it to the new EU-wide framework on cybersecurity. Additional measures on standards, certification and labelling to ensure that connected objects are more secure are proposed. (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN)
Agenda

• Definitions and taxonomy of critical infrastructure
• National cyber security strategies
• Critical infrastructure security incidents
• Threats
• Vulnerabilities
• The NIST Framework for Improving Critical Infrastructure Cybersecurity
• From security to resilience
INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID
Summary of the Incident

• On December 23, 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company, reported service outages to customers. The outages were due to a third party’s illegal entry into the company’s computer and SCADA systems: Starting at approximately 3:35 p.m. local time, seven 110 kV and 23 35 kV substations were disconnected for three hours.

• The outages were originally thought to have affected approximately 80,000 customers, based on the Kyivoblenergo’s update to customers. However, later it was revealed that three different distribution oblenergos (a term used to describe an energy company) were attacked, resulting in several outages that caused approximately 225,000 customers to lose power across various areas.

• Shortly after the attack, Ukrainian government officials claimed the outages were caused by a cyber attack, and that Russian security services were responsible for the incidents.

Attack highlights

- Spear phishing to gain access to the business networks of the oblenergos
- Identification of BlackEnergy 3 at each of the impacted oblenergos
- Theft of credentials from the business networks
- The use of virtual private networks (VPNs) to enter the ICS network
- The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI
- Serial-to-ethernet communications devices impacted at a firmware level
- The use of a modified KillDisk to erase the master boot record of impacted organization systems as well as the targeted deletion of some logs
- Utilizing UPS systems to impact connected load with a scheduled service outage
- Telephone denial-of-service attack on the call center
Belgacom Attack

Britain's GCHQ Hacked Belgian Telecoms Firm

A cyber attack on Belgacom raised considerable attention last week. Documents leaked by Edward Snowden and seen by SPIEGEL indicate that Britain's GCHQ intelligence agency was responsible for the attack.
Summary of the incident

- In September 2013, the German magazine *Der Spiegel* reported, based on documents leaked by Edward Snowden, that GCHQ operatives had hacked the computers of Belgacom employees, gaining access to Belgacom’s network, as well as to Belgacom International Carrier Services (BICS), the subsidiary that provides phone and internet traffic in Africa and the Middle East.

- The information was provided by GCHQ to intelligence services in New Zealand, Canada, Australia and the US, which, with the UK, make up the group known as Five Eyes.

- The new revelations show that the initial hacking – codenamed Operation Socialist – took place before June 2011 and was more extensive than Belgacom has so far admitted. Contrary to Belgacom’s previous claims, the hacking gave GCHQ access via BICS to virtually every mobile number in Europe, the Middle East and Africa. It wasn’t just private clients of Belgacom who were under surveillance, but also the telephone networks of Nato and the EU in Brussels, as well as international delegations and embassies.

Source: [https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/](https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/)
Attack highlights

- In-depth reconnaissance, to covertly map out the company’s network and identify key employees in areas related to maintenance and security.
- Monitored the browsing habits of the engineers, and launched a “Quantum Insert” attack, which involves redirecting people targeted for surveillance to a malicious website that infects their computers with malware.
- The malware platform used was Regin (also known as Prax or WarriorPride).
Hackers Launch All-Out Assault on Norway's Oil and Gas Industry

August 31, 2014 // 05:17 PM EST

In what's being billed as the largest ever coordinated cyberattack in Norway, hackers have targeted some 300 different firms within the country's oil and energy industries. The attacks were revealed last week by the Nasjonal Sikkerhetsmyndighet (National Security Authority Norway), which had been tipped off to the attacks by "international
Summary of the incident

• Nearly 300 Norwegian companies in the oil and energy industry have been warned by state authorities about the largest coordinated hacker attack reported in the country. This warning comes after reports of 50 oil companies hacked, including Statoil, the largest oil company in the country, according to the national security authority, NSM (Nasjonal Sikkerhetsmyndighet).

Source: https://duo.com/blog/norway-s-oil-companies-targets-of-largest-coordinated-attack
Attack highlights

- The NSM reported the attacks are being conducted via well-researched phishing campaigns, that is, emails directed at certain employees with key privileges and functions within the companies, such as system operators. If the email attachments are opened by employees, attackers can execute a program and scan their network for security holes; after finding one, attackers can set up malware.

- After installing malware, attackers can use a keylogger to log keyboard strokes and credentials that allow them to continue to effectively work their way through the network.
Hack attack causes 'massive damage' at steel works

© 22 December 2014  Technology

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace.
Summary of the incident

• In December, 2014 the German government’s Bundesamt für Sicherheit in der Informationstechnik (BSI) (translated as Federal Office for Information Security) released their annual findings report.
• In one case they noted that a malicious actor had infiltrated a steel facility. The adversary used a spear phishing email to gain access to the corporate network and then moved into the plant network.
• According to the report, the adversary showed knowledge in ICS and was able to cause multiple components of the system to fail. This specifically impacted critical process components to become unregulated, which resulted in massive physical damage.
• To date, the only other public example of a cyber attack causing physical damage to control systems was Stuxnet.

Attack highlights

- According to the report the exploitation of the German steel mill took place by targeting on-site personnel in the corporate network. The BSI report also stated that the targeted group were industrial operators.
- Adversaries targeted the personnel with spear phishing emails. Recent ICS-targeted technical threats have included this style of targeting with phishing emails as was observed in the HAVEX and BlackEnergy campaigns.
- Targeting and delivery techniques have focused on specific individuals, trusted relationships with ICS and industrial suppliers, and the need to download files.
UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

By Russell Bordan | @russelbrandton | May 12, 2017, 11:30am EDT
Summary of the incident

• The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.
• It propagated through EternalBlue, an exploit in older Windows systems released by The Shadow Brokers a few months prior to the attack. WannaCry also took advantage of installing backdoors onto infected systems.
• The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars.
• In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was behind the attack.
• A new variant of WannaCry ransomware forced Taiwan Semiconductor Manufacturing Company (TSMC) to temporarily shut down several of its chip-fabrication factories in August 2018. The virus spread to 10,000 machines in TSMC’s most advanced facilities.

Source: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
Attack highlights

• The attack began on Friday, 12 May 2017, with evidence pointing to an initial infection in Asia at 07:44 UTC. The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed. Within a day the code was reported to have infected more than 230,000 computers in over 150 countries.

• When executed, the WannaCry malware first checks the "kill switch" domain name; if it is not found, then the ransomware encrypts the computer's data, then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet, and "laterally" to computers on the same network. As with other modern ransomware, the payload displays a message informing the user that files have been encrypted, and demands a payment of around $300 USD in bitcoin within three days, or $600 USD within seven days. Three hardcoded bitcoin addresses, or "wallets", are used to receive the payments of victims.
The Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploit
- Installation
- Command and Control (C&C)
- Action
FY 2016 Incidents by Sector (290 total)

- Defense Industrial Base, 1
- Financial Services, 2
- Emergency Services, 2
- Food and Agriculture, 3
- Chemical, 4
- Commercial Facilities, 5
- Nuclear Reactors, Materials and Waste, 7
- Information Technology, 7
- Healthcare and Public Health, 11
- Transportation Systems, 14
- Dams, 0

Source:
https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf
FY 2016 Incidents by Threat Vector (290 total)

- Removable Media, 1
- Rogue Device, 1
- Brute Force, 3
- Abuse of Authorized Access, 5
- SLQ, 7
- Network Scanning/Probing, 35

- Unknown, 82
- Other, 36
- Weak Authentication, 43
- Spear Phishing, 77
Agenda

• Definitions and taxonomy of critical infrastructure
• National cyber security strategies
• Critical infrastructure security incidents
• Threats
• Vulnerabilities
• The NIST Framework for Improving Critical Infrastructure Cybersecurity
• From security to resilience
Figure 3: the elements of a risk and their relationships according to ISO 15408:2005

Source: ENISA Threat Landscape 2015
“If you know your enemies and know yourself, you will not be imperiled in a hundred battles”, Sun Tzu, The Art of War, 6th century BC
Cybersecurity Threat Agents

Source: 2013 ENISA Threat Landscape, Figure 20: Overview of Agents in Cyber Space.
Threat taxonomies: The ENISA taxonomy

- **High level threats**: this is the top level threat category, used mainly to discriminate families of threats.
- **Threats**: this field indicates the various threats within a category.
- **Threats details**: in this field details of a specific threat are being described. Threat details are based on a specific attack type/method or targeting specific IT asset.

Source: ENISA Threat Taxonomy 2016
## Trends

<table>
<thead>
<tr>
<th>Top Threats 2016</th>
<th>Assessed Trends 2016</th>
<th>Top Threats 2017</th>
<th>Assessed Trends 2017</th>
<th>Change in ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Malware</td>
<td>![Upward Arrow]</td>
<td>1. Malware</td>
<td>![Downward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>2. Web based attacks</td>
<td>![Upward Arrow]</td>
<td>2. Web based attacks</td>
<td>![Downward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>3. Web application attacks</td>
<td>![Upward Arrow]</td>
<td>3. Web application attacks</td>
<td>![Downward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>4. Denial of service</td>
<td>![Upward Arrow]</td>
<td>4. Phishing</td>
<td>![Downward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>5. Botnets</td>
<td>![Neutral Arrow]</td>
<td>5. Spam</td>
<td>![Upward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>6. Phishing</td>
<td>![Neutral Arrow]</td>
<td>6. Denial of service</td>
<td>![Downward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>7. Spam</td>
<td>![Neutral Arrow]</td>
<td>7. Ransomware</td>
<td>![Upward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>11. Exploit kits</td>
<td>![Neutral Arrow]</td>
<td>11. Data breaches</td>
<td>![Upward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>12. Data breaches</td>
<td>![Neutral Arrow]</td>
<td>12. Identity theft</td>
<td>![Upward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>13. Identity theft</td>
<td>![Neutral Arrow]</td>
<td>13. Information leakage</td>
<td>![Upward Arrow]</td>
<td>→</td>
</tr>
<tr>
<td>15. Cyber espionage</td>
<td>![Neutral Arrow]</td>
<td>15. Cyber espionage</td>
<td>![Downward Arrow]</td>
<td>→</td>
</tr>
</tbody>
</table>

Legend: Trends: ![Declining], ![Stable], ![Increasing]

Ranking: ![Going up], ![Same], ![Going down]

Source: ENISA Threat Landscape 2017
Agenda

- Definitions and taxonomy of critical infrastructure
- National cyber security strategies
- Critical infrastructure security incidents
- Threats
- Vulnerabilities
- The NIST Framework for Improving Critical Infrastructure Cybersecurity
- From security to resilience
Cyber vulnerabilities

- In FY 2016, ICS-CERT identified 700 weaknesses through its 98 DAR (Design Architecture Reviews) and NAVV (Network Validation and Verification) assessments. The top 30 categories of weaknesses, make up roughly 79 percent of all identified weaknesses.

Who is the weakest security link?
If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

https://www.schneier.com/books/secrets_and_lies/pref.html
A structured, holistic approach is needed
Agenda

- Definitions and taxonomy of critical infrastructure
- National cyber security strategies
- Critical infrastructure security incidents
- Threats
- Vulnerabilities
- The NIST Framework for Improving Critical Infrastructure Cybersecurity
- From security to resilience
The NIST Framework for Improving Critical Infrastructure Cybersecurity

- Includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

- Provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

- Identifies areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations.

- Is consistent with voluntary international standards.
The Framework is for organizations...

- Of any size, in any sector in (and outside of) the critical infrastructure.
- That already have a mature cyber risk management and cybersecurity program.
- That don’t yet have a cyber risk management or cybersecurity program.
- Needing to keep up-to-date managing risks, facing business or societal threats.
International Use
Framework for Improving Critical Infrastructure Cybersecurity

- Japanese translation by Information-technology Promotion Agency
- Italian adaptation within Italy’s National Framework for Cybersecurity
- Hebrew adaptation by Government of Israel
- Bermuda uses it within government and recommends it to industry
- Uruguay government is currently on Version 3.1 of their adaptation
- Focus of International Organization for Standardization & International Electrotechnical Commission
Cybersecurity Framework Components

### Framework Core
- Aligns industry standards and best practices to the Framework Core in a particular implementation scenario.
- Supports prioritization and measurement while factoring in business needs.

### Framework Profile
- Describes how cybersecurity risk is managed by an organization and the degree to which the risk management practices exhibit key characteristics defined in the core.

### Framework Implementation Tiers
- Cybersecurity activities and informative references, organized around particular outcomes.
- Enables communication of cyber risk across an organization.
The Framework Core...

- ...is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
  - **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
  - **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
  - **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
  - **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
  - **Recover** - Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

- The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.
The Framework Core
Core Cybersecurity Framework Component

Senior Executives
- Broad enterprise considerations
- Abstracted risk vocabulary

Specialists in Other Fields
- Specific focus outside of cybersecurity
- Specialized or no risk vocabulary

Implementation/Operations
- Deep technical considerations
- Highly specialized vocabulary
## Core
### Cybersecurity Framework Component

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Asset Management</td>
<td>ID.AM</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
<td>ID.BE</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>ID.GV</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
<td>ID.RA</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
<td>ID.RM</td>
</tr>
<tr>
<td>Protect</td>
<td>Access Control</td>
<td>PR.AC</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
<td>PR.AT</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
<td>PR.DS</td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes &amp; Procedures</td>
<td>PR.IP</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>PR.MA</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td>PR.PT</td>
</tr>
<tr>
<td></td>
<td>Anomalies and Events</td>
<td>DE.AE</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
<td>DE.CM</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>DE.DP</td>
</tr>
<tr>
<td>Respond</td>
<td>Response Planning</td>
<td>RS.RP</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RS.CO</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
<td>RS.AN</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>RS.MI</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RS.IM</td>
</tr>
<tr>
<td>Recover</td>
<td>Recovery Planning</td>
<td>RC.RP</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RC.IM</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RC.CO</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>ID</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Identify</td>
<td>Asset Management</td>
<td>ID.AM</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
<td>ID.BE</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>ID.GV</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
<td>ID.RA</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
<td>ID.RM</td>
</tr>
<tr>
<td>Protect</td>
<td>Access Control</td>
<td>PR.AC</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
<td>PR.AT</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
<td>PR.DS</td>
</tr>
<tr>
<td></td>
<td>Information Protection</td>
<td>PR.IP</td>
</tr>
<tr>
<td></td>
<td>Processes &amp; Procedures</td>
<td>PR.IP</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>PR.MA</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td>PR.PT</td>
</tr>
<tr>
<td></td>
<td>Anomalies and Events</td>
<td>DE.AE</td>
</tr>
<tr>
<td></td>
<td>Security Continuous</td>
<td>DE.CM</td>
</tr>
<tr>
<td></td>
<td>Monitoring</td>
<td>DE.CM</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>DE.DP</td>
</tr>
<tr>
<td></td>
<td>Response Planning</td>
<td>RS.RP</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RS.CO</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
<td>RS.AN</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>RS.MI</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RS.IM</td>
</tr>
<tr>
<td></td>
<td>Recovery Planning</td>
<td>RC.RP</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RC.IM</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RC.CO</td>
</tr>
</tbody>
</table>

### Subcategory: Identify

| ID.BE-1: | The organization’s role in the supply chain is identified and communicated |
|          | \[COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2, NIST SP 800-53 Rev. 4 CP-2, SA-12\] |
| ID.BE-2: | The organization’s place in critical infrastructure and its industry sector is identified and communicated |
|          | \[COBIT 5 APO02.06, APO03.01, NIST SP 800-53 Rev. 4 PM-8\] |
| ID.BE-3: | Priorities for organizational mission, objectives, and activities are established and communicated |
|          | \[COBIT 5 APO02.01, APO02.06, APO03.01, ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6, NIST SP 800-53 Rev. 4 PM-11, SA-14\] |
| ID.BE-4: | Dependencies and critical functions for delivery of critical services are established |
|          | \[ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3, NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14\] |
| ID.BE-5: | Resilience requirements to support delivery of critical services are established |
|          | \[COBIT 5 DSS04.02, ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1, NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14\] |
The Framework Implementation Tiers…

• … provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.
• Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive).
• The Tiers characterize an organization’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.
• During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.
The Framework Implementation Tiers

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Partial</td>
<td>Risk Informed</td>
<td>Repeatable</td>
<td>Adaptive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Risk Management Process</strong></th>
<th>The functionality and repeatability of cybersecurity risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrated Risk Management Program</strong></td>
<td>The extent to which cybersecurity is considered in broader risk management decisions</td>
</tr>
<tr>
<td><strong>External Participation</strong></td>
<td>The degree to which the organization benefits by sharing or receiving information from outside parties</td>
</tr>
</tbody>
</table>
The Framework Implementation Tiers...

- **Tier 1: Partial**
  - **Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
  - **Integrated Risk Management Program** – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
  - **External Participation** – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.
The Framework Implementation Tiers…

• Tier 2: Risk Informed
  – Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
  – Integrated Risk Management Program – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
  – External Participation – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.
The Framework Implementation Tiers…

• **Tier 3: Repeatable**
  - **Risk Management Process** – The organization’s risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
  - **Integrated Risk Management Program** – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
  - **External Participation** - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community’s broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.
The Framework Implementation Tiers…

- **Tier 4: Adaptive**
  - **Risk Management Process** – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.
  - **Integrated Risk Management Program** – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.
  - **External Participation** - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community’s broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.
A Framework Profile (“Profile”)…

• ...represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories.
• The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.
• Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state).
• To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization’s risks.
• The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost effectiveness and innovation.
• Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.
Profile

Ways to think about a Profile:

• A customization of the Core for a given sector, subsector, or organization.

• A fusion of business/mission logic and cybersecurity outcomes.

• An alignment of cybersecurity requirements with operational methodologies.

• A basis for assessment and expressing target state.

• A decision support tool for cybersecurity risk management.
Building a Profile
A Profile Can be Created in Three Steps

1. Mission
   - Objective
     - A
     - B
     - C

2. Cybersecurity Requirements
   - Legislation
   - Regulation
   - Internal & External Policy
   - Best Practice

3. Operating Methodologies
   - Guidance and methodology on implementing, managing, and monitoring

Subcategory
- 1
- 2
- 3
- ...
- 98
When you organize yourself in this way:

- Compliance reporting becomes a byproduct of running your security operation
- Adding new security requirements is straightforward
- Adding or changing operational methodology is non-intrusive to on-going operation
Resource and Budget Decision Making

What Can You Do with a CSF Profile?

<table>
<thead>
<tr>
<th>Sub-category</th>
<th>Priority</th>
<th>Gaps</th>
<th>Budget</th>
<th>Year 1 Activities</th>
<th>Year 2 Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>moderate</td>
<td>small</td>
<td>$$$</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>high</td>
<td>large</td>
<td>$$</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>moderate</td>
<td>medium</td>
<td>$</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>moderate</td>
<td>none</td>
<td>$$</td>
<td>reassess</td>
<td></td>
</tr>
</tbody>
</table>

...and supports on-going operational decisions, too
Coordination of Framework Implementation

Risk Management

Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities

Business/Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget

Mission Priority and Risk Appetite and Budget

Implementation

Implementation/Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Framework Profile

Changes in Current and Future Risk

Implementation Progress Changes in Assets, Vulnerability and Threat
How to Use the Framework

- Basic Review of Cybersecurity Practices
- Establishing or Improving a Cybersecurity Program
  - Step 1: Prioritize and Scope
  - Step 2: Orient
  - Step 3: Create a Current Profile
  - Step 4: Conduct a Risk Assessment
  - Step 5: Create a Target Profile
  - Step 6: Determine, Analyze, and Prioritize Gaps
  - Step 7: Implement Action Plan
- Communicating Cybersecurity Requirements with Stakeholders
- Buying Decisions
- Identifying Opportunities for New or Revised Informative References
- Methodology to Protect Privacy and Civil Liberties
Applying the Cybersecurity Framework at the University of Chicago - Background

- The Biological Sciences Division (BSD), with 5,000 faculty and staff in 23 departments, is the largest division of the university. These departments support basic research, clinical research, education, and patient care led by award-winning faculty. These functions, including groundbreaking discoveries in fields such as cancer research and advanced genomics, are enabled by an array of information technology resources.
Applying the Cybersecurity Framework at the University of Chicago – The challenge

- The BSD supports an array of information technology resources that enable faculty, staff and students to advance their research and education.
- This support is supplied through a decentralized model using local Information Technology staff, hired to fulfill specific departments’ technology needs.
- This model provides departments with the agility to support research projects with unique Information Technology requirements. However, autonomous Information Technology resources within departments, each with its own management and governance processes, results in the following security challenges:
  - risks due to inconsistent applications of security controls;
  - risks due to gaps in security controls across departments;
  - increase in spending on security; and,
  - duplication of effort.
Applying the Cybersecurity Framework at the University of Chicago – Approach

**BSD Cybersecurity Framework Implementation Approach**

- **Current State**
  - Identify priorities
  - Determine compliance requirements
  - Review existing policies and practices
  - Identify vulnerabilities and risk events

- **Assessment**
  - Identify threats
  - Review vulnerabilities
  - Define probability and likelihood
  - Categorize identified risks
  - Create risk heat map

- **Target State**
  - Identify mitigation approaches
  - Translate mitigation into desired outcomes
  - Define goals for desired outcomes
  - Review and outline security priorities

- **Roadmap**
  - Quantify and score current state
  - Establish budget and identify resources
  - Define targets within budget
  - Share results with stakeholders

**Continuous Improvement**
Applying the Cybersecurity Framework at the University of Chicago – Stage 1

- Interviews of key stakeholders (Information Technology (IT) staff, business managers and executive leadership)
- Identification of the priorities of individual departments.
  - current and planned security activities across the BSD,
  - requirements for sharing research information remotely, and
  - the need to support faculty activities in day-to-day research and education.
- A customized Current Profile template was used to create an internal management tool that documents existing policies, tools in use, and examples of good BSD practices. This information established the BSD’s Cybersecurity Framework Current Profile.
Applying the Cybersecurity Framework at the University of Chicago – Stage 2

• Several hundred vulnerabilities that resulted from profile development were considered, and a set of unique threats that could conceivably impact operations was subsequently identified.
• The likelihood and potential impact of each risk was determined.
• The risk events were aggregated into points of commonality, creating a comprehensive register of risk categories (e.g. financial, operational, and strategic).
• The combined risk categories were plotted on a Heat Map.
Applying the Cybersecurity Framework at the University of Chicago – Stage 3

- High-level approaches to mitigate each of the documented risks were determined.
- A Cybersecurity Framework Implementation Tier was selected.
- The risk mitigation approaches were translated into desired outcomes, using the Target State Profile categories and subcategories as a guide.
- The combination of these activities established the BSD’s Cybersecurity Framework Target Profile.
Applying the Cybersecurity Framework at the University of Chicago – Stage 4

• A rating scale from 0 to 4 (derived from ISO 15504) was used to quantify the current state and to establish a baseline.

• Goals were determined based on the operational budget, resources, and competing priorities. These goals were plotted on top of the current state in the example radar chart.

NB: ISO/IEC 33001 has replaced ISO 15504 since 2015
Applying the Cybersecurity Framework at the University of Chicago – Continuous Improvement

• Framework Assessment Collaboration Tool (FACT).
• Provides information for periodic self-assessment by departments, supporting questionnaires regarding current and planned activities for department staff, external partners, information security processes, security tools, training systems, etc.
• Provides a consolidated view of how individual departments are meeting the cybersecurity targets set for the specific fiscal year.
• Most importantly, the information gained is used to improve and mature the cybersecurity program in alignment with the BSD’s business objectives.
Agenda

• Definitions and taxonomy of critical infrastructure
• National cyber security strategies
• Critical infrastructure security incidents
• Threats
• Vulnerabilities
• The NIST Framework for Improving Critical Infrastructure Cybersecurity
• From security to resilience
Is complete protection possible?

- “If there are two or more ways to do something, and one of those ways can result in a catastrophe, then someone will do it”; or
- Anything that can go wrong will go wrong.

Edward Aloysius Murphy Jr. (January 11, 1918 – July 17, 1990)
From Protection to Resilience (1)

- Complete protection can never be guaranteed (may be cost – inefficient).
- “A resilient infrastructure is a component, system or facility that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored.” (CIIP Resilience Series Monograph, George Mason University 2007).
From Protection to Resilience (2)

• A good example of resilience in practice comes from the London Underground and bus bombings in July 2005. The very next day, the trains and buses were running again and the city was open for business as usual – thanks to prior resilience plans.

• By contrast, hurricane Katrina in New Orleans in 2005 is an example of lack of resilience. The telecommunications infrastructure in the affected area was not only disrupted (e.g. due to power blackouts) but was completely destroyed.
A final note…

“Those who surrender freedom for security will not have, nor do they deserve, either one.”

Benjamin Franklin, 1706-1790
Thank you!