CYBERSECURITY AS PART OF DIGITAL STRATEGY

CyberShare Conference,
IAŞI, 24/5/2019

AGENDA

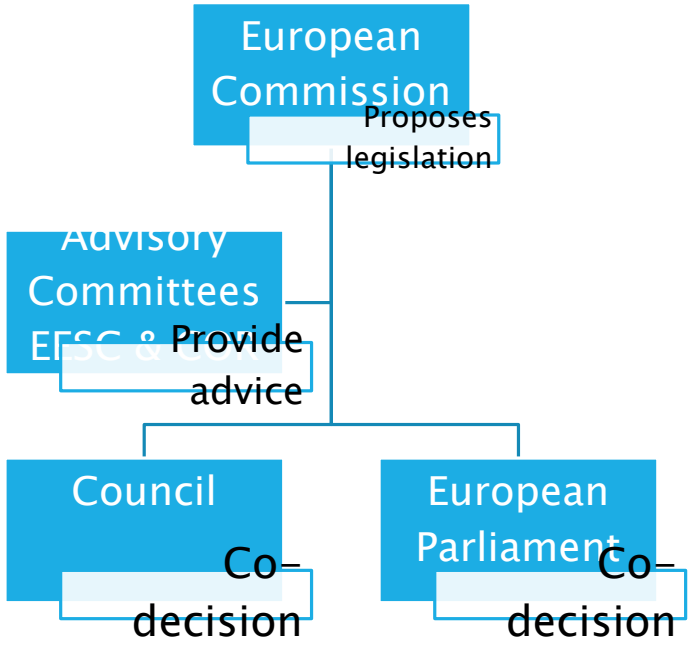
1. Background
2. IT and Digital Strategy
3. Cybersecurity and the Threat Landscape
4. Conclusions and Bibliography

AGENDA

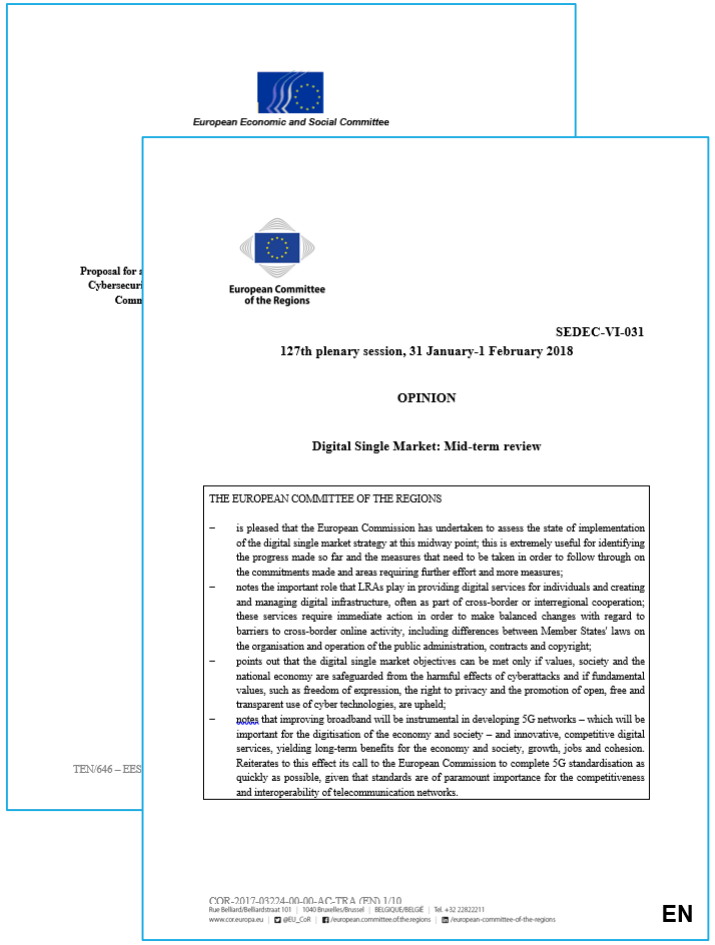
1. **Background**
2. IT and Digital Strategy
3. Cybersecurity and the Threat Landscape
4. Conclusions and Bibliography

BACKGROUND

1. “The European Parliament, the Council and the Commission shall be assisted by an **Economic and Social Committee** and a **Committee of the Regions** acting in an advisory capacity.” Treaty on European Union, Article 13
2. The **European Economic and Social Committee** (EESC) ensures that civil society organisations have a say in Europe's development
3. The **European Committee of the Regions** (CoR) represents local and regional authorities across the European Union and advises on new laws that have an impact on regions and cities (70% of all EU legislation).



Decisions


European Economic and Social Committee

European Committee of the Regions

SEDEC-VI-031

127th plenary session, 31 January-1 February 2018

OPINION

Digital Single Market: Mid-term review

THE EUROPEAN COMMITTEE OF THE REGIONS

- is pleased that the European Commission has undertaken to assess the state of implementation of the digital single market strategy at this midway point; this is extremely useful for identifying the progress made so far and the measures that need to be taken in order to follow through on the commitments made and areas requiring further effort and more measures;
- notes the important role that LRAs play in providing digital services for individuals and creating and managing digital infrastructure, often as part of cross-border or interregional cooperation; these services require immediate action in order to make balanced changes with regard to barriers to cross-border online activity, including differences between Member States' laws on the organisation and operation of the public administration, contracts and copyright;
- points out that the digital single market objectives can be met only if values, society and the national economy are safeguarded from the harmful effects of cyberattacks and if fundamental values, such as freedom of expression, the right to privacy and the promotion of open, free and transparent use of cyber technologies, are upheld;
- notes that improving broadband will be instrumental in developing 5G networks – which will be important for the digitisation of the economy and society – and innovative, competitive digital services, yielding long-term benefits for the economy and society, growth, jobs and cohesion. Reiterates to this effect its call to the European Commission to complete 5G standardisation as quickly as possible, given that standards are of paramount importance for the competitiveness and interoperability of telecommunication networks.

EN

Opinions

Members

romania2019.eu

Activitățile **CESE**
în timpul **Președinției române**

Ianuarie – iunie 2019

Comitetul Economic şi Social European

1994 2019
Comitetul European al Regiunilor

Comitetul European al Regiunilor și Președinția României la Consiliul Uniunii Europene

DELEGAȚIA ROMÂNIEI LA CoR

romania2019.eu

AGENDA

1. Background
2. **IT and Digital Strategy**
3. Cybersecurity and the Threat Landscape
4. Conclusions and Bibliography

IT AT THE COMMITTEES

1. IT is a service shared by the EESC and the COR
2. Governed by a Cooperation Agreement
3. Common objectives and challenges:
   - ✓ High quality of service
   - ✓ Fair & balanced approach
   - ✓ Proactive
   - ✓ Financial efficiency
   - ✓ Sustainable
   - ✓ Accountability & transparency
   - ✓ Well being at work


EUROPEAN UNION
Committee of the Regions
European Economic and Social Committee

ADMINISTRATIVE COOPERATION AGREEMENT

BETWEEN

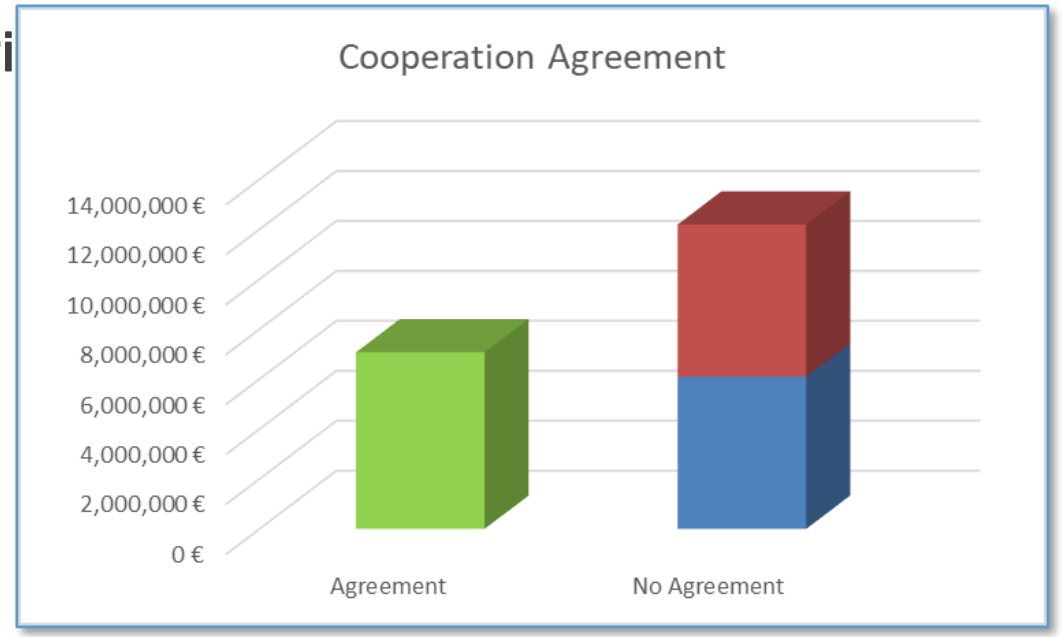
THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE

AND

THE COMMITTEE OF THE REGIONS

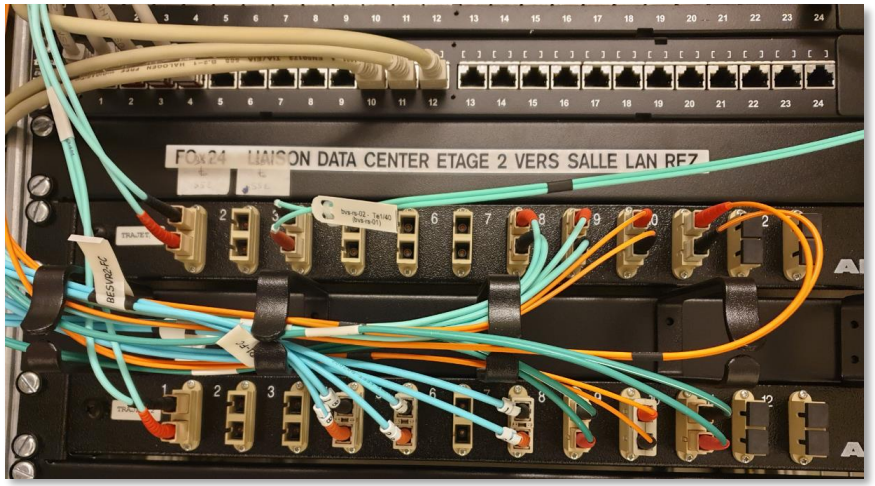
IT SYNERGIES

- ✓ Annual IT budget of some 7M€ ≡ 3% of total budget
- ✓ Estimated annual savings of some 40% percent
- ✓ In addition to savings due to general inter-institutional cooperation **including IT securi**



IN PRACTICE

1. In practical terms, IT:
   - ✓ Develops & maintains information systems
   - ✓ Runs the data centre
   - ✓ Operates the data & voice network
   - ✓ Manages **IT security**
   - ✓ Supports users & solves their problems



DIGITAL STRATEGY

1. General Framework
   - Principles behind the vision (digital by default, **security & privacy** …)
   - **Digital workplace** (devices, office automation, mail and calendars ….)
   - Strengthening **Cybersecurity**
2. Strategic projects
   - Focus on filling gaps in the political domain
3. Enablers
   - Governance, Budget & **Digital Skills**

DIGITAL STRATEGY PRINCIPLES

The underlying principles supporting the Digital Strategies of the European Institutions are based on those of the EU e-Government Action Plan, the European Interoperability Framework (EIF) and the Tallinn Declaration:

a. Digital by Default & Once Only

b. Openness & Transparency

c. Interoperability & Cross-border

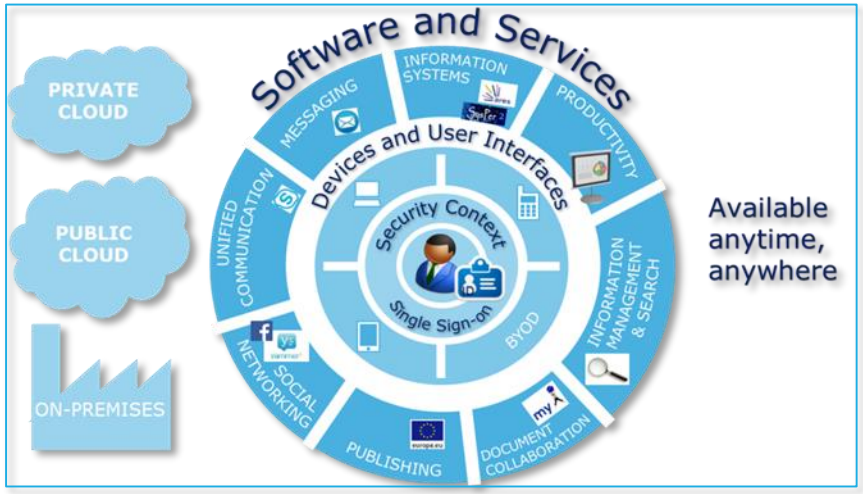
d. Security & Privacy

e. User-driven, Data-centric and Agile design

DIGITAL WORKPLACE PRINCIPLES

Digital Workplace

… Deploy a 'Secure-By-Design' infrastructure … advanced security measures will be embedded within the design of the Digital Workplace components, achieving a quantum leap in our security posture …



AGENDA

1. Background
2. IT and Digital Strategy
3. **Cybersecurity and the Threat Landscape**
4. Conclusions and Bibliography

STRENGTHENING CYBERSECURITY

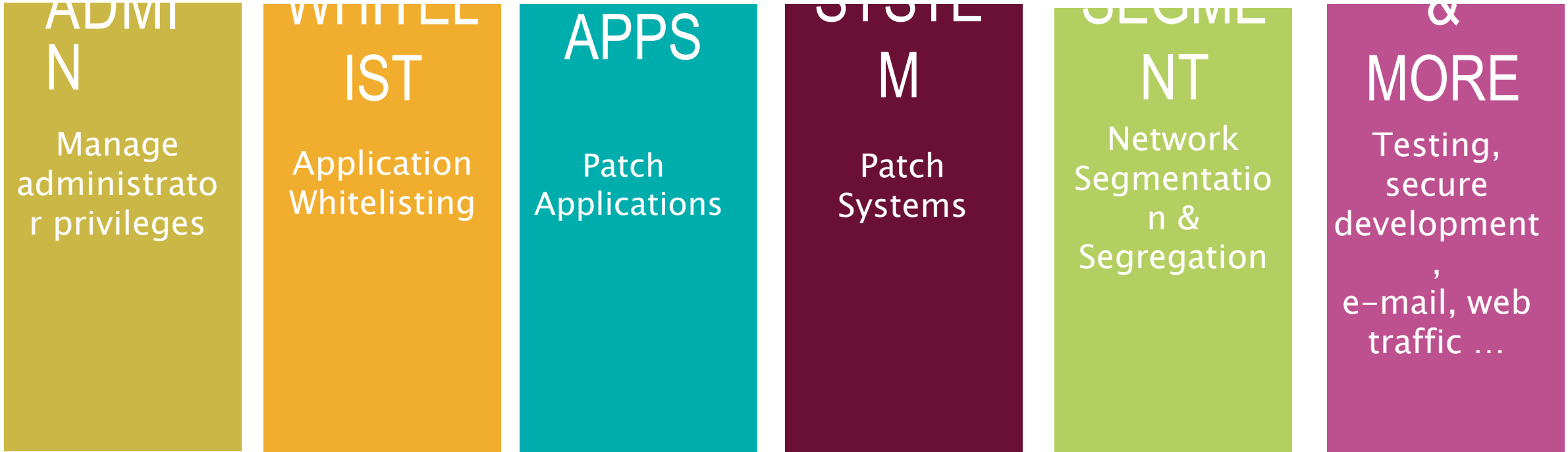
IT Security deliverables within the Digital Strategy:

- ✓ Establish a very solid security baseline
- ✓ Increase detection and response capabilities
- ✓ Adopt a risk-based approach
- ✓ Keep IT Security within the scope of IT Governance
- ✓ Increase endpoint security
- ✓ Train and raise awareness among users
- ✓ Pursue cooperation with CERT-EU (*)
- ✓ Maintain, and regularly test, the recovery plan

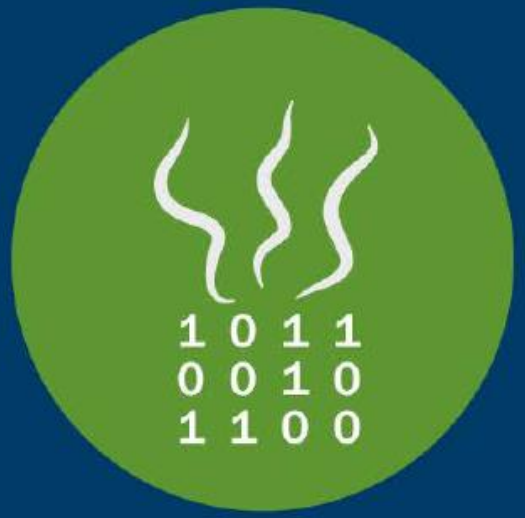
(*) The CERT of the EU institutions, agencies & bodies

SECURITY BASELINE

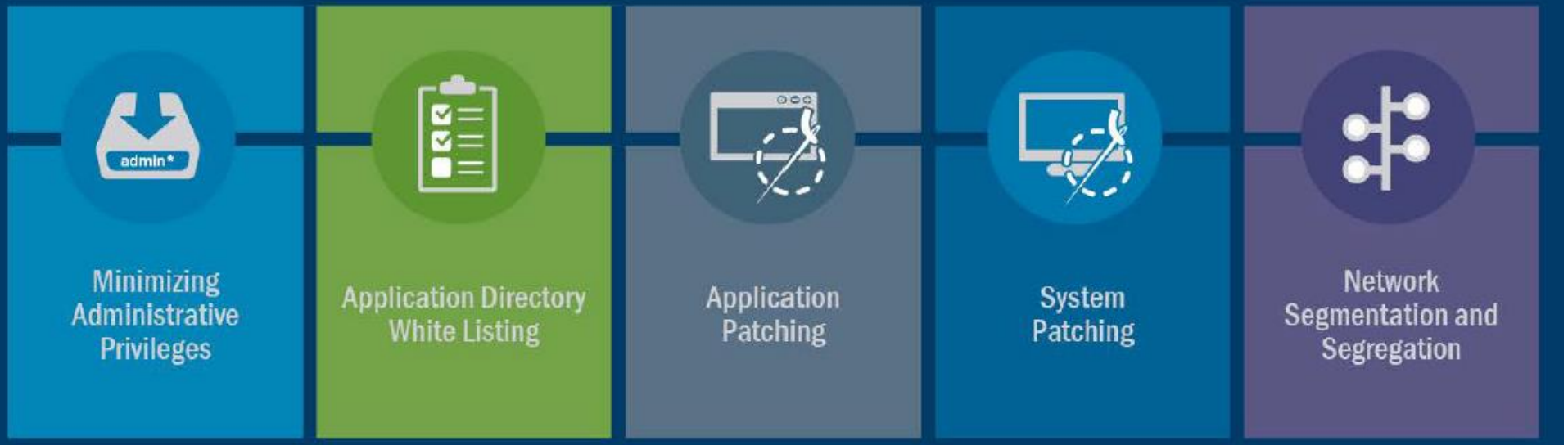
- ✓ Constant attention to maintain the security baseline at a high level
- ✓ The objective is to **prevent** a high percentage of cyber attacks



MITIGATION
BASIC CYBER HYGIENE "US-CERT Top 5"



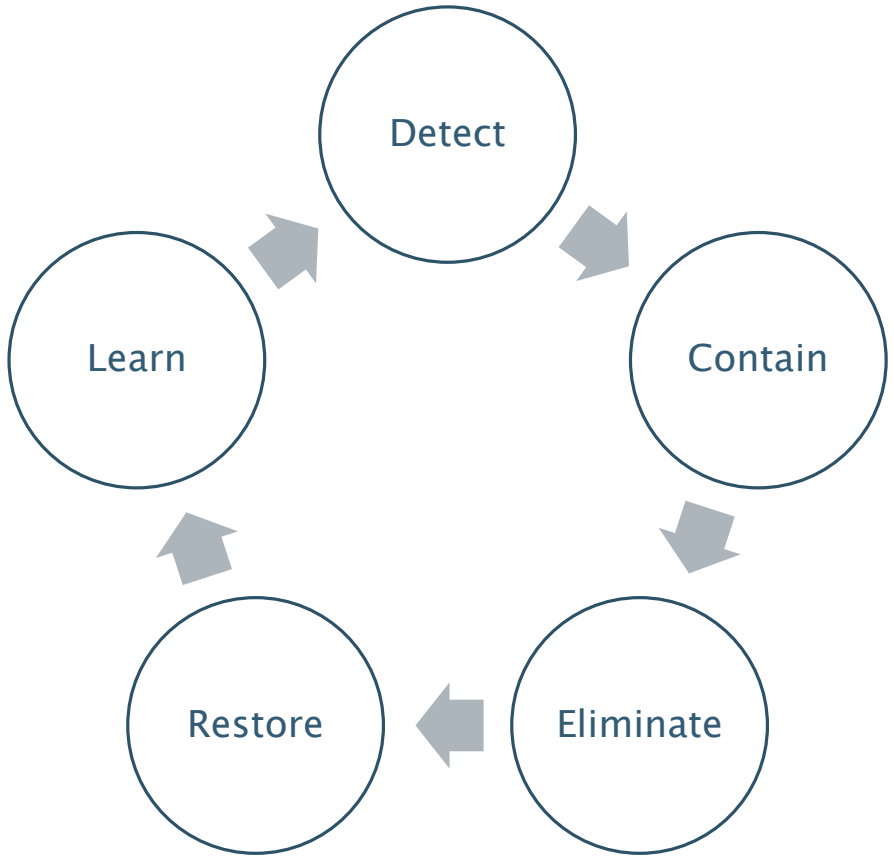
Basic cyber hygiene would prevent approximately 85% of the security breaches security practitioners deal with today.



From "Best Practices & Common Missteps in Responding to Major Incidents",

INCREASE DETECTION AND RESPONSE CAP

- ✓ Use a wide range of tools for detection including actionable alerts from CERT-EU,
- ✓ Centralised security log-file management & incident management procedure,
- ✓ The objective is to be able to **detect** advanced cyberattacks in a timely manner.



ADOPT A RISK BASED APPROACH

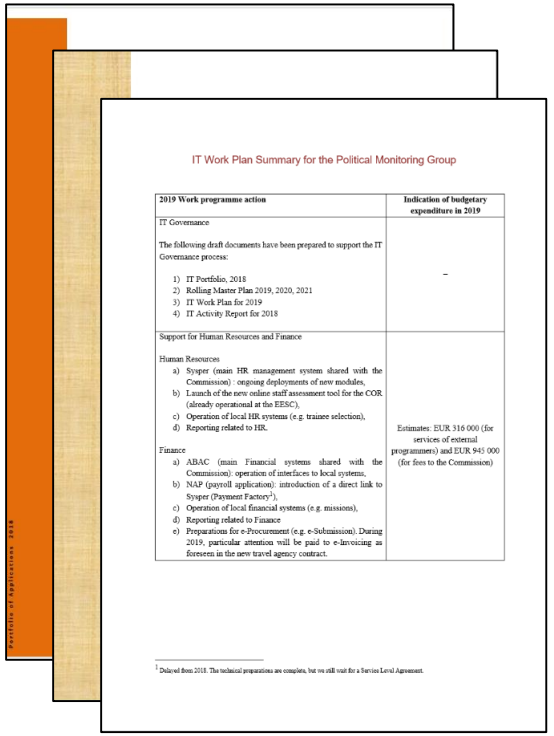
- ✓ Annual risk assessment + continuous reporting prepared by **IT Security Officer**,
- ✓ Security plans prepared with **Business Owners**,
- ✓ Need to prepare for **cloud** deployments (later GovSec Cloud),
- ✓ The objective is the ongoing adoption of Risk Management **best practices**.

IT Risk Table 2019

#	IT Asset	Threat-Source	Impact	Existing controls	Probability	Risk Level	Further Controls/Comments
1	Workstations (Browsers, Office Software etc)	Unauthorized external users (e.g. ,hackers) get access to user's workstation and install malicious software	Medium	Browser security settings, Antivirus, Antispyware, Workstation patching	Medium	Low	

GOVERNANCE

- ✓ **IT Steering Committees** decide on planning, resources & priorities
- ✓ IT Security is part of this process (assessment of the threat landscape, follow-up of previous work plan and adoption of the current work plan)
- ✓ The objective is to leverage the existing structure and to **keep IT Security within the scope of IT Governance**



IT Work Plan Summary for the Political Monitoring Group

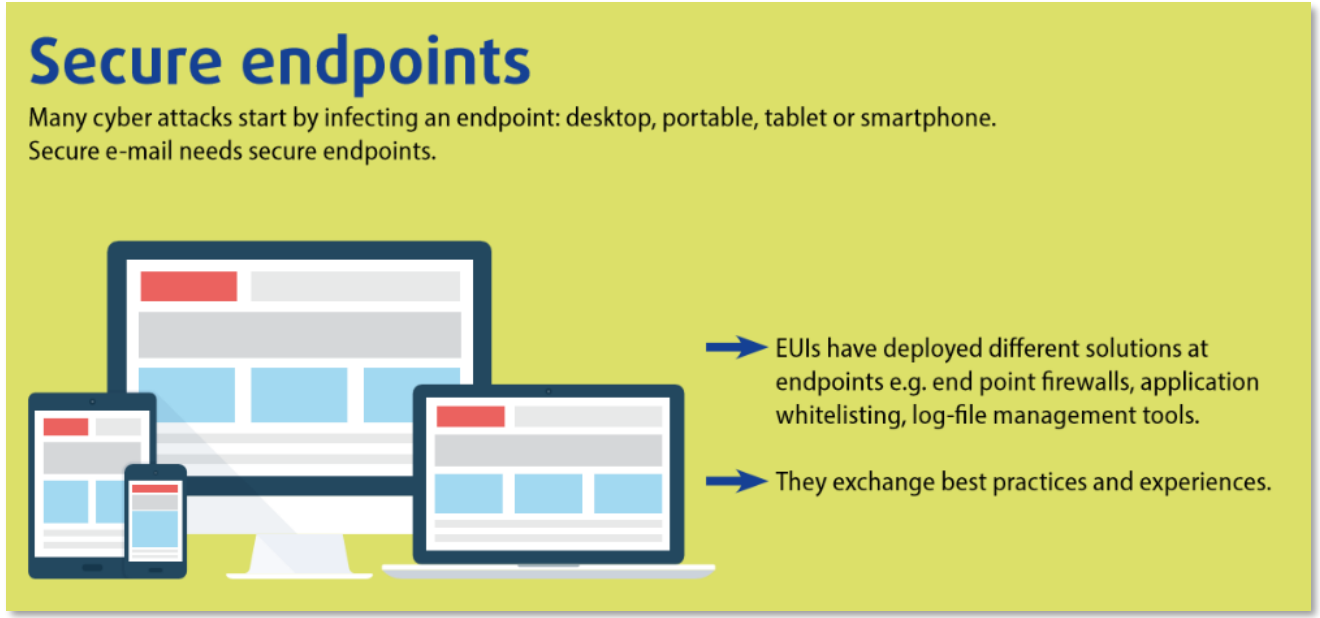
2019 Work programme action	Indication of budgetary expenditure in 2019
IT Governance The following draft documents have been prepared to support the IT Governance process: 1) IT Portfolio, 2018 2) Rolling Master Plan 2019, 2020, 2021 3) IT Work Plan for 2019 4) IT Activity Report for 2018	-
Support for Human Resources and Finance Human Resources a) Sysper (main HR management system shared with the Commission) : ongoing deployments of new modules, b) Launch of the new online staff assessment tool for the COR (already operational at the EESC), c) Operation of local HR systems (e.g. trainee selection), d) Reporting related to HR. Finance a) ABAC (main Financial systems shared with the Commission): operation of interfaces to local systems, b) NAP (payroll application): introduction of a direct link to Sysper (Payment Factory[1]), c) Operation of local financial systems (e.g. missions), d) Reporting related to Finance e) Preparations for e-Procurement (e.g. e-Submission). During 2019, particular attention will be paid to e-Invoicing as foreseen in the new travel agency contract.	Estimates: EUR 316 000 (for services of external programmers) and EUR 945 000 (for fees to the Commission)

[1] Delayed from 2018. The technical preparations are complete, but we still wait for a Service Level Agreement.

...

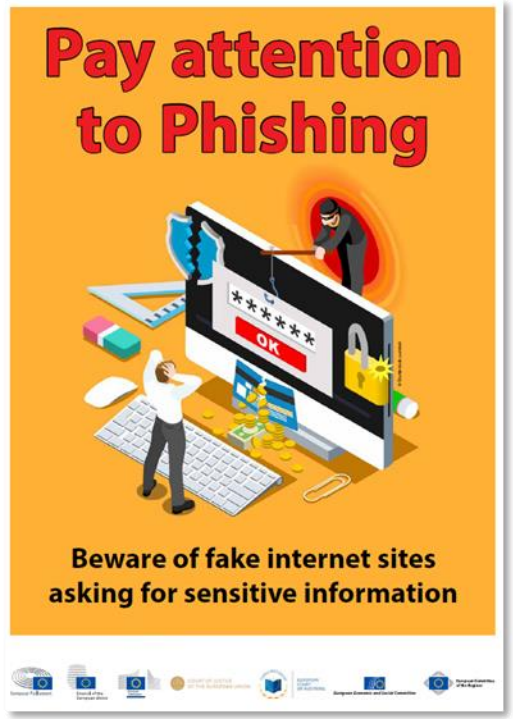
IMPROVE ENDPOINT SECURITY

- ✓ Ongoing rollout of new security features as part of the **“one PC”** programme
- ✓ VPN with one-time passwords for remote connections
- ✓ Advanced threat protection and MFA depending on the risk



AWARENESS RAISING

- ✓ Communicate regularly on IT security topics
- ✓ Organise practical events and exercises
- ✓ Good cooperation in this domain based on:
  - **Content** (benchmarking, coordinating campaigns) &
  - **Channels**(sharing, speaker panels and joint activities)
- ✓ The objective is to be **practical & to measure progress.**



COOPERATION

The Committees benefit from the services of CERT-EU :

- ✓ Value-added services – e.g. external vulnerability scanning and penetration testing,
- ✓ Opportunity to participate in innovative projects – e.g. threat hunting project,
- ✓ Broader cooperation horizons – e.g. participation in cyber exercises and coordinated response to major incidents,
- ✓ The objective is to **maintain & deepen this cooperation**.

RECOVERY PLAN

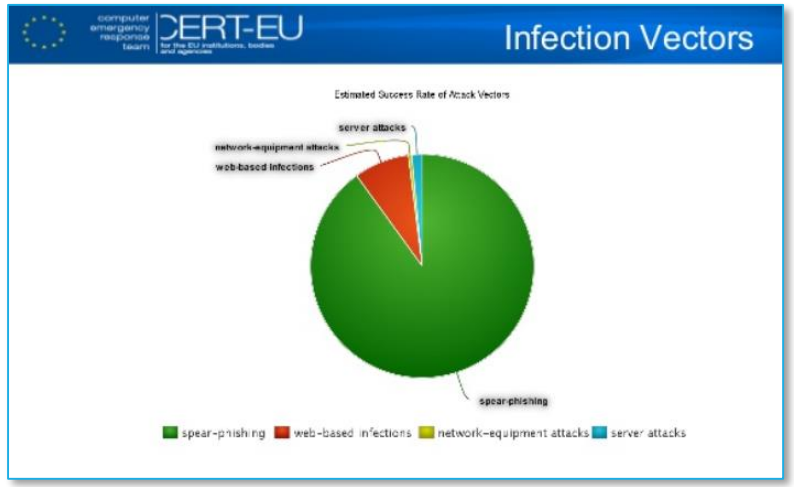
The Committees have an established Business Continuity Plan:

- ✓ To ensure “critical and essential functions” during crises,
- ✓ To return to “business as usual” as quickly as possible,
- ✓ Under the responsibility of a Crisis Management Team,
- ✓ The objective is to **work closely with the Crisis Management Team.**

THREAT LANDSCAPE

The Committees use the threat awareness material from CERT-EU:

- ✓ Operational (e.g. Incident Reports, Advisories, Feeds)
- ✓ Tactical (e.g. TTPs, Ongoing campaigns, Whitepapers based on incidents)
- ✓ Strategic (e.g. Security Brief, Threat Landscape),
- ✓ Including early warning capacities.



AGENDA

1. Background
2. IT and Digital Strategy
3. Cybersecurity and the Threat Landscape
4. **Conclusions and Bibliography**

CONCLUSIONS

Digital Strategies reinforce cybersecurity by:

- ✓ Setting objectives to continuously improve security position while,
- ✓ Taking into account the **Threat Landscape** &
- ✓ Fostering a **Shared Responsibility** approach.

BIBLIOGRAPHY

1. Referenced in the presentation

[01] The Tallinn Declaration on e-Government, 6/10/2017
http://ec.europa.eu/newsroom/document.cfm?doc_id=47559

[02] European Commission Digital Workplace Strategy
https://ec.europa.eu/info/publications/digital-workplace-strategy_en

[03] CERT-EU
https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html

BIBLIOGRAPHY

[04] Best Practices and Common Missteps in responding to Major Incidents
Chris Butera, Chief of Incident Response, US-CERT
https://www.first.org/resources/papers/conf2016/FIRST-2016-108.pdf

[05] GovSEC Cloud Blueprints for secure governance of cloud computing
ISA² Programme
https://ec.europa.eu/isa2/actions/making-usage-cloud-safer_en

[06] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises. C/2017/6100
https://publications.europa.eu/en/publication-detail/-/publication/e7f7a728-9cff-11e7-b92d-01aa75ed71a1/language-en/format-PDFA1A

BIBLIOGRAPHY

2. Other references

[07] Digital Single Market: Mid-term review, 31/01/2018, COR Opinion https://cor.europa.eu/en/our-work/Pages/OpinionTimeline.aspx?opId=CDR-3224-2017

[08] Cybersecurity Act, 14/02/2018, EESC Opinion https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/cybersecurity-act

[09] The European Committee of the Regions and the Romanian Presidency of the Council of the European Union https://cor.europa.eu/en/engage/brochures/Pages/default.aspx?from=01/01/2019&to=01/01/2020

[10] The EESC's activities during the Romanian Presidency. January – June 2019 https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/eescs-activities-during-romanian-presidency-january-june-2019