asee

by asseco

Cyber Crime: The Invisible Business Risk

Slobodan Maksimović

Belgrade, 2025

asee by asseco

State of Cybercrime

The Damage & Costs Continue to Rise

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Cybercrime Magizine

Data loss and downtime is increasingly prevalent

52%

of orgs have suffered a cyberattack in the last 12 months

75%

concerned their existing data protection may not be sufficient to cope with malware and ransomware threats

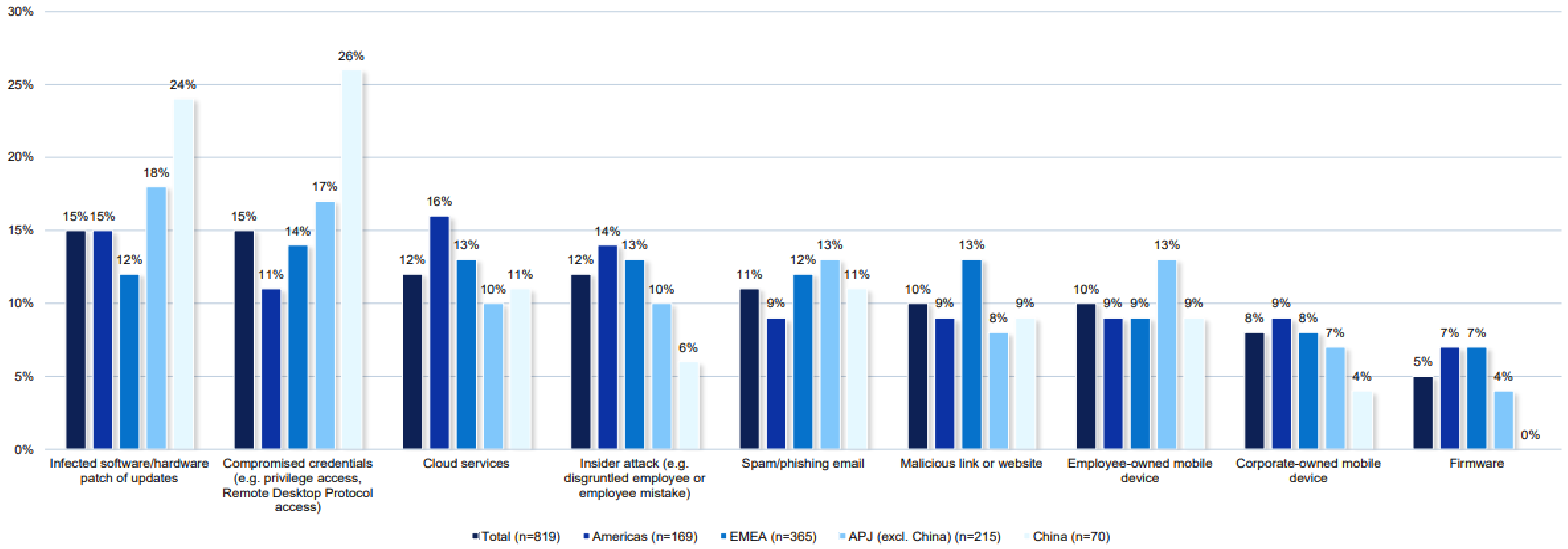
85%

that experienced a ransomware attack, paid to access their data asee by asseco

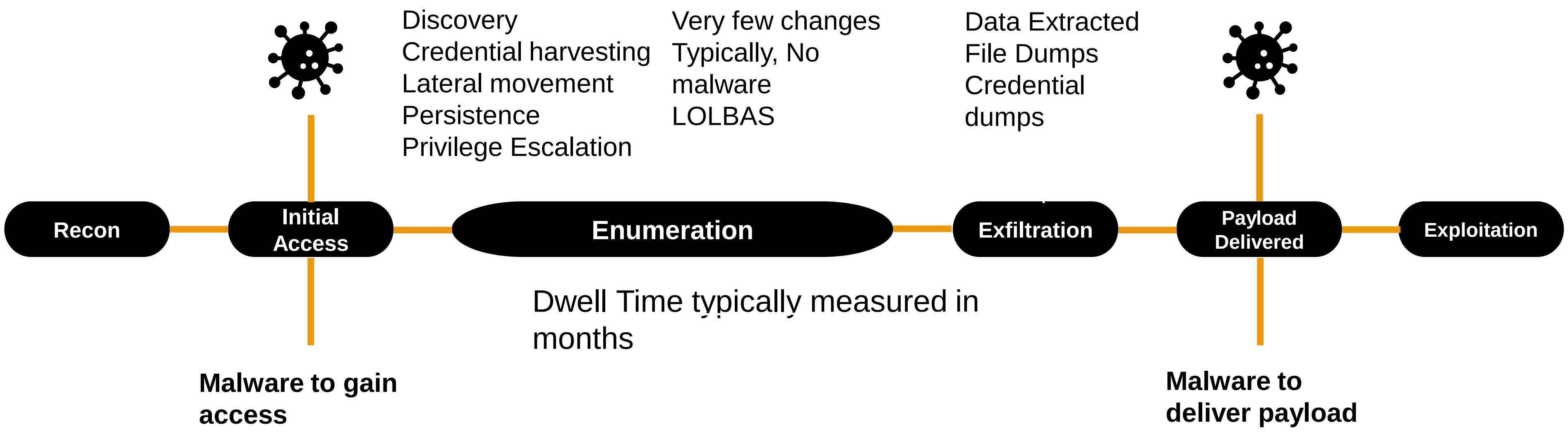
Global Data Protection Index - 2024

Cyber criminals target various entry points, with attacks more likely to come from external sources

Entry point for organization's most recent cyberattack, split by region



Anatomy of a Cyber Attack



Detection of Malware is difficult
Attacks typically comes as a single big bang

Operational Change

Maverick Research: You Will Be Hacked, So Embrace the Breach

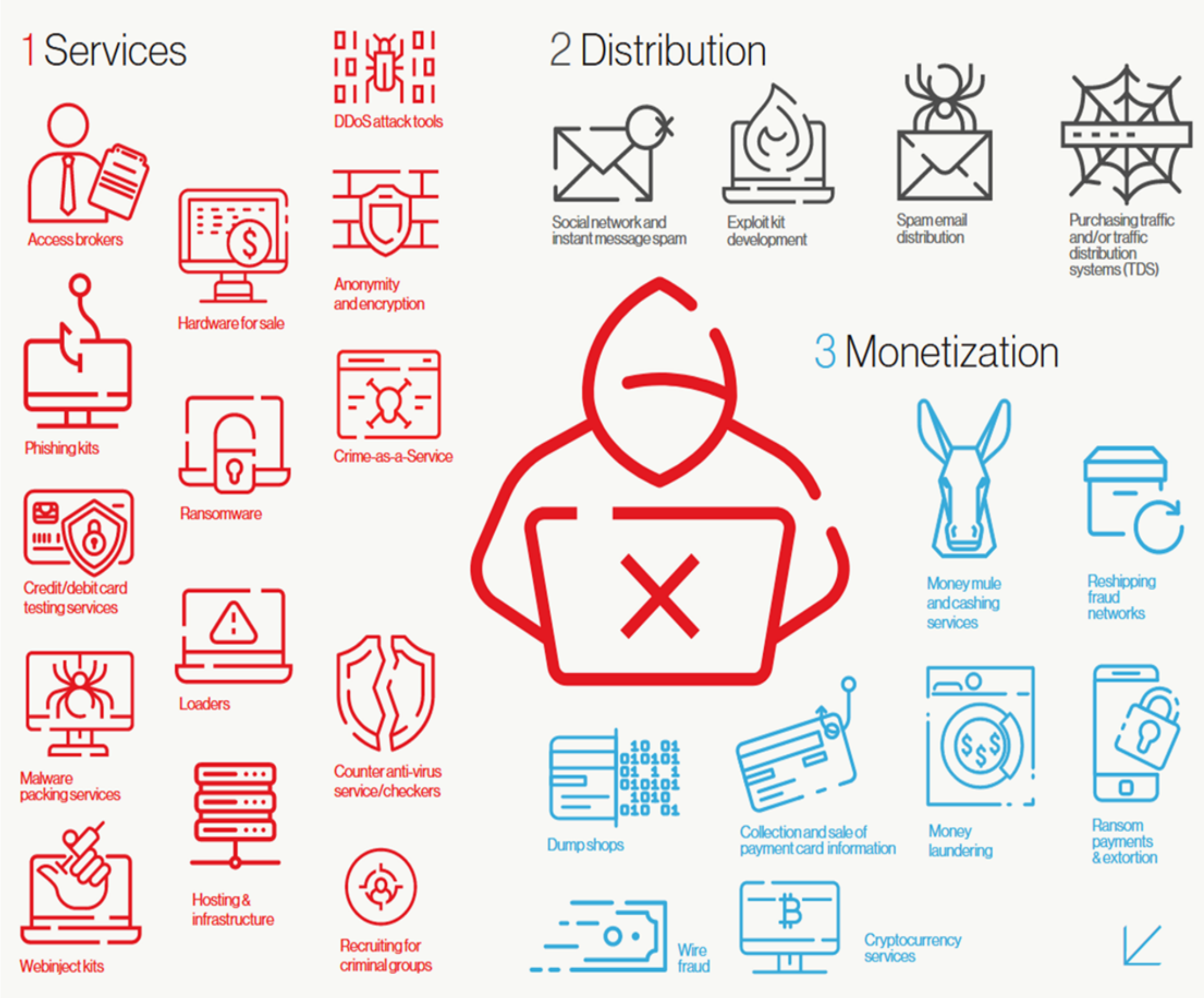
"Cybersecurity breaches are inevitable, but many security and risk management leaders still think they can prevent all hacks by throwing people and money at their defenses. Instead of striving so hard to prevent breaches, they should focus on resilience and embrace hacks as incidents to learn from."

– Gartner

It’s not IF….

but When

Events once seen as extreme and unusual are now commonplace.



(Digital Operational Resilience Act)

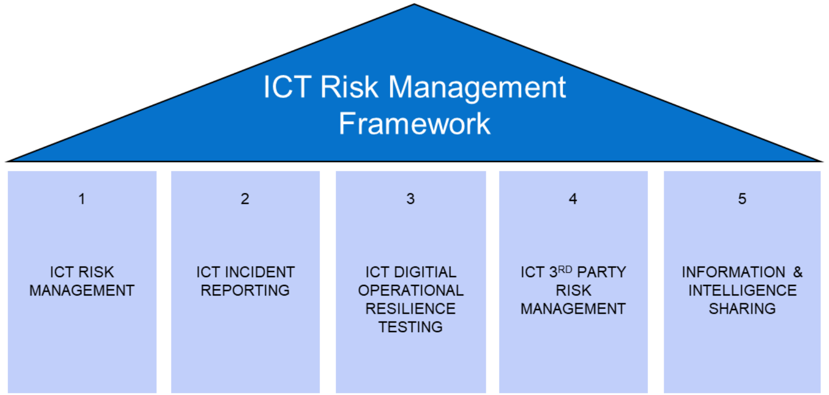
DORA

Jan 16th, 2023, DORA in force

period: Jan 17th 2025

Test the ICT business continuity plans and the ICT response and recovery plans at least yearly.

Use ICT systems that are physically and logically segregated from the source ICT system



Penalties

- ***Financial institutions not fixed – member states determine***
- ***Potential criminal sanctions***
- ***ICT providers: 1% of average worldwide turnover in proceeding year, applied daily until compliance is achieved for 6 months***

DORA - Digital Operational Resilience Act

Article 12, Backup policies and procedures, restoration and recovery procedures and methods

1. For the purpose of ensuring the restoration of ICT systems and data with minimum downtime, limited disruption and loss, as part of their ICT risk management framework, financial entities shall develop and document:
   a) backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data
   b) restoration and recovery procedures and methods
2. Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardise the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically.
3. When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorised access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary (…)
4. Financial entities, other than microenterprises, shall maintain redundant ICT capacities equipped with resources, capabilities and functions that are adequate to ensure business needs (…)
6. In determining the recovery time and recovery point objectives for each function, financial entities shall take into account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.
7. When recovering from an ICT-related incident, financial entities shall perform necessary checks, including any multiple checks and reconciliations, in order to ensure that the highest level of data integrity is maintained. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.

NIS2

- NIS2 supersedes the first NIS (Network and Information Security) Directive, adopted in July 2016.
- Member States have until Q3/Q4 2024 to become compliant.

- Administrative fines up to €10m or 2% annual worldwide turnover
- Liability of top managers and C-Level executives within the organizations.
  - → Suspension of certifications and authorizations for services or activities provided by the organization
  - → A temporary ban from management positions within the entity for any person discharging managerial responsibilities at chief executive officer or legal representative level.
- The NIS2 Directive strengthens security requirements in the EU
- It expands its scope to more sectors and entities
- Taking into account the security of supply chains
- Streamlining reporting obligations
- Introducing monitoring measures
- Introducing more stringent enforcement requirements
- Harmonizing and tightening sanctions in all Member States

Who Does NIS2 Apply To?

- Understand which sectors and organizations are affected by NIS2

Essential Entities (EE)

Size threshold: varies by sector, but generally 250 employees, annual turnover of € 50 million or balance sheet of € 43 million

- Energy
- Transport
- Finance
- Public Administration
- Health
- Space
- Water supply (drinking & wastewater)
- Digital Infrastructure

Important Entities (IE)

Size threshold: varies by sector, but generally 50 employees, annual turnover of € 10 million or balance sheet of € 10 million

- Postal Services
- Waste Management
- Chemicals
- Research
- Foods
- Manufacturing
- Digital Providers

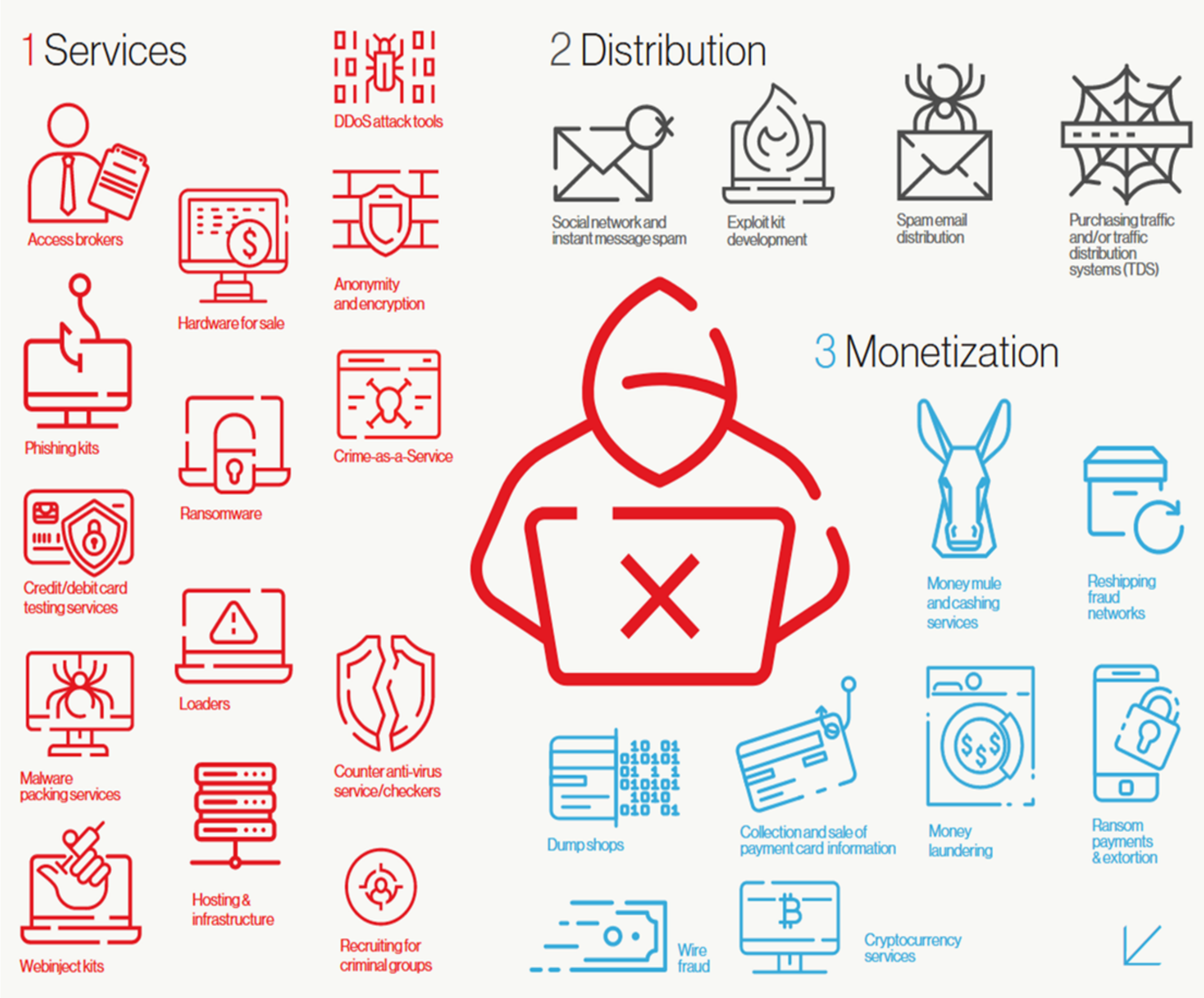
How to protect

- Network & Perimeter Security
- Identity, Access & Privileged Security
- Endpoint & Extended Detection
- Network Detection & Response (NDR)
- Data Protection & Backup (Anti-Ransomware)
- Cloud Security & Container Security
- Email & Collaboration Security
- SIEM, Monitoring & Observability
- Governance, Risk & Compliance
- **Employee Education**

It's not IF….

but **When**

Events once seen as extreme and unusual are now commonplace.



Thank you

http:// asee.io