Cisco
Customer Experience

Regulations inbound

NIS2, DORA et al: What do they mean for the way we conduct business?

Tim (Wadhwa-)Brown, Security Consulting Senior Engineering Technical Leader

CX CoE Security

Regulatory updates

- UK
  - Telecom Security Act
  - Data Protection and Digital Information Bill
  - Online Safety Bill
  - Updates to Network and Information Systems Regulations (NIS Regulations)?
  - Reform of Computer Misuse Act?

- European
  - **NIS2 Directive**
  - European Cyber Resilience Act
  - **Digital Operational Resilience Act (DORA)**
  - Critical Entities Resilience Directive (CER)
  - Digital Services Act (DSA)
  - Digital Markets Act (DMA)
  - European Chips Act
  - European Data Act
  - European Data Governance Act (DGA)
  - EU Cyber Solidarity Act
  - Artificial Intelligence Act
  - Artificial Intelligence Liability Directive
  - European ePrivacy Regulation
  - European Digital Identity Regulation
  - ...

NIS2: A quick summary

- **Risk assessments and security policies** for information systems
- **Policies and procedures for evaluating security measures** and their efficacy
- **Policies and procedures for us cryptography** and, when re encryption
- **Plan for handling security inci ents** including detection, response and recovery
- **Security around the procurement of systems** and the development and operation of systems
- **Cyb security training** and a practice for omputer hygiene
- **procedures for employees with ss to sensitive or important data**, cluding policies for data access
- **Plan for managing business operations** during and after a security incident
- **Use of multi-factor authentication**, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication
- **Security around supply chains** and the relationship between the company and direct supplier.

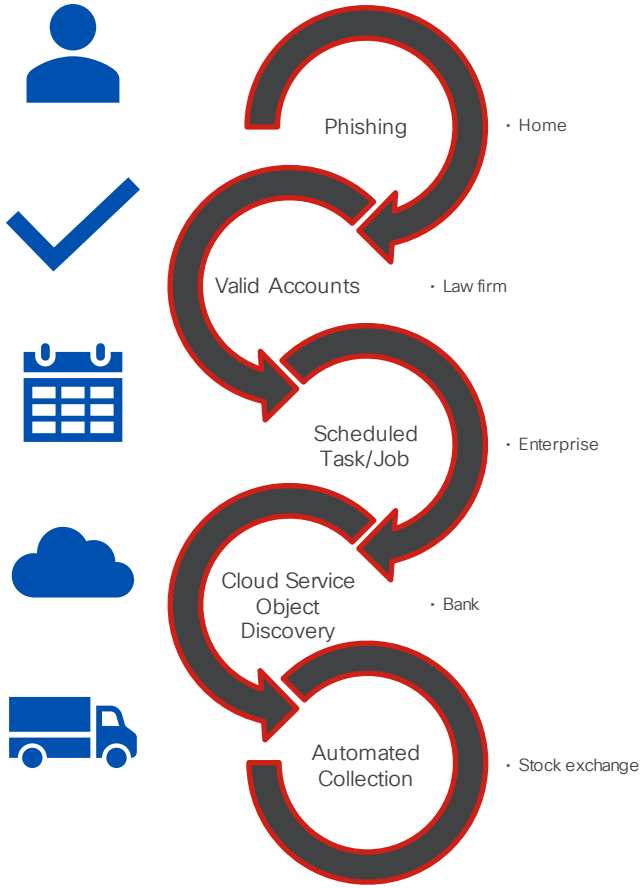
Taken from article 21: Cybersecurity risk-management measures

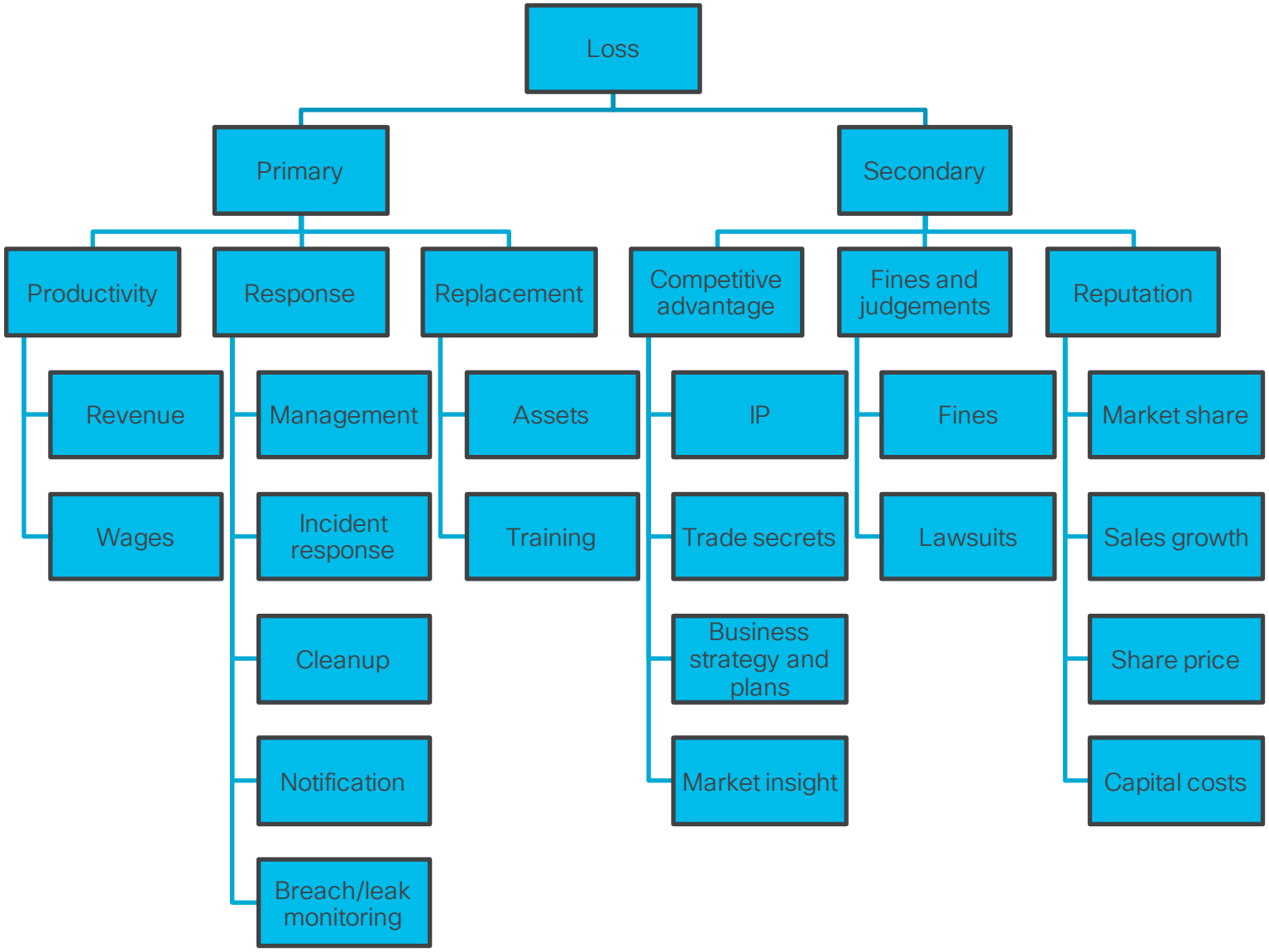
Threat landscape

Why these regulations are necessary

Worst case scenarios

- Technical failure
  - CNI networks
  - 3rd party systems
    - Payment networks
    - Telecoms networks
- Financial failure
- Societal failure
- Cyber
  - State
  - Terrorism
  - Criminal





Regulation necessary to address market gaps

NIS2 etc will force organisations to address externalities inherited from 3rd parties

Addressing risk

- I am not your lawyer :)
- 2 bears
  - Regulator
  - Threats
- Everyone's a third party for someone these days
  - Hybrid working
  - SaaS
  - Digitisation of everyday life
- Risks can be inherited

- Significant incidents
  - Cause or are capable of causing severe operational disruption of the services or financial loss for the entity concerned
  - Has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage
- Fines from the competent authority
  - Essential entities: Up to €10000000 or 2% of the global yearly revenue, with the higher amount being applicable
  - Important entities: Up to €7000000 or 1.4% of the annual global revenue, with the higher amount being applicable

3rd party risk by numbers

- On average, organisations share confidential information with around 583 third parties*
  - 34% of respondents admitted to maintaining comprehensive inventories
  - 63% of respondents believed they lacked resources to manage third-party relationships
  - Only 35% rated their third-party risk management programs as highly effective

* Taken from Data Risk in the Third-Party Ecosystem study by the Ponemon Institute, 2018

Considerations

- Direct will depend on the nature of the essential entity…
  - Impact of every day goods and services
  - Impact of market places
  - Impact of communications
  - Impact of utilities
  - Imagine losing your water or food supply…
- Indirect
  - Impact of cross-border arrangements
  - Impact of emergencies, societal failure etc
  - Impact of Internet access and public communications networks
  - Impact of managed service providers
  - Impact of DNS services
  - Impact of CDN providers
  - Impact of cloud services
  - Impact of data centres
  - Impact of supply chain
  - Impact of managed security service providers
  - Onwards dependencies

Even for UK businesses, expect to see regulatory changes and increased contractual pressures...

Constructing a NIS2 strategy

Avoiding piecemeal implementation

Metrics that matter

- Requirements
  - An early warning within 24 hours of becoming aware of the significant incident
  - An incident notification within 72 hours of becoming aware of the significant incident
  - Upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates
  - A final report not later than one month after the submission of the incident notification
- Operational capabilities
  - Mean time to detect
  - Mean time to respond

Hygiene Is critical

- Be honest with your customers and suppliers
- Cyber Essentials
  - https://www.ncsc.gov.uk/section/products-services/cyber-essentials
- Exercise in a Box
  - https://www.ncsc.gov.uk/information/exercise-in-a-box
- Procurement
  - https://www.ncsc.gov.uk/collection/supply-chain-security

Aim for secure-by-design

- Prioritize investment
  - Operational – tomorrow
  - Tactical – next 6 months
  - Strategic – 18 months
- Engage with the ecosystem
  - https://www.cisco.com/c/en/us/about/trust-center/trust-portal/security-risk-assessment.html
- Ensure you consider your own 3rd party risks

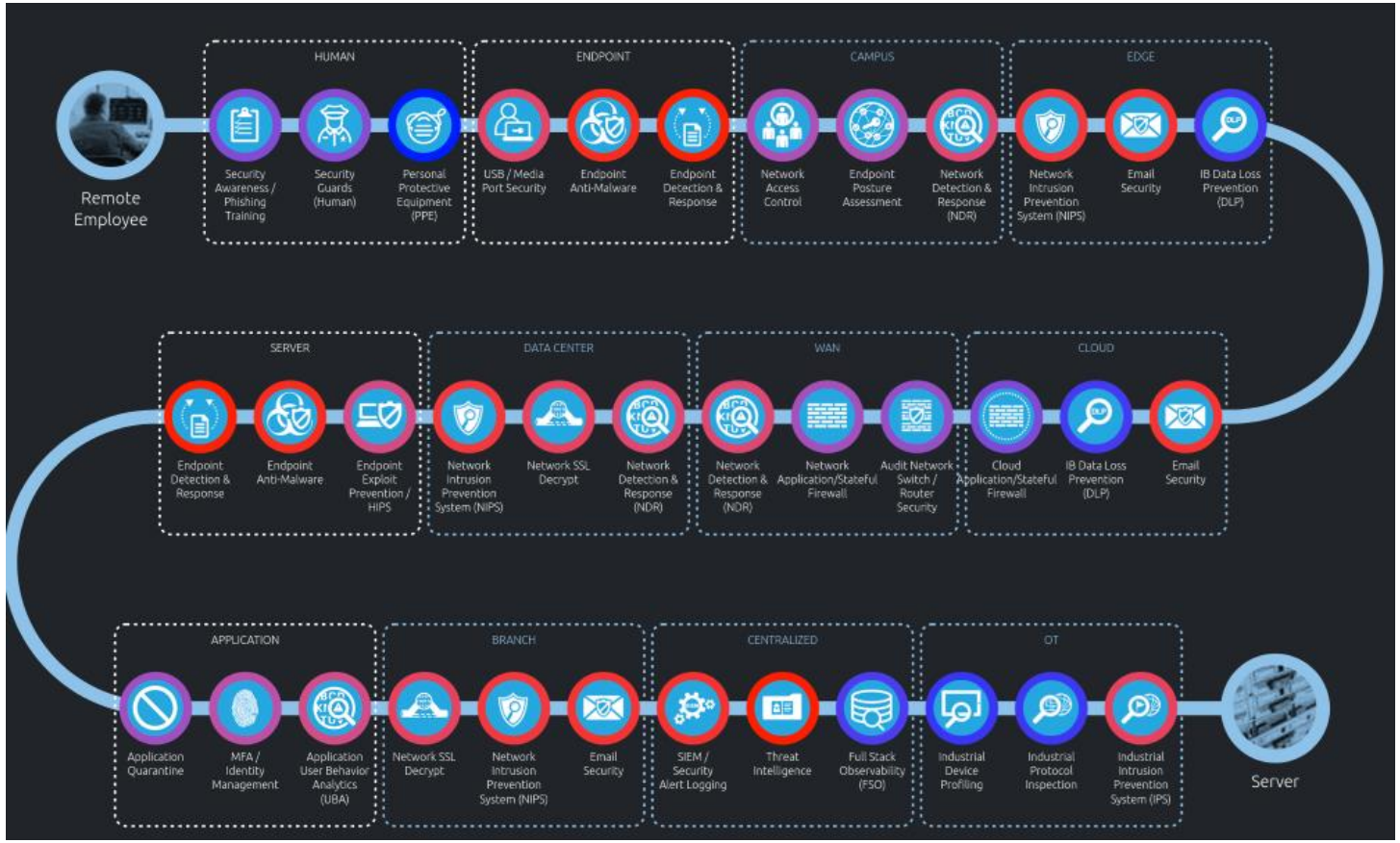
Adopt security principles and patterns

- NCSC's Cyber Assessment Framework
  - https://www.ncsc.gov.uk/collection/caf
- Principles of zero trust
  - No implicit trust
  - Strongly authenticated user
  - Strongly authenticated device
  - Encrypted connection to resource
  - Policy decision and enforcement

Understand your threat model

- Ask yourself
  - What would happen if another pandemic hit?
  - What about ransomware?
  - Do I support any critical customers?
  - Do I know how to contact the regulator?
  - What revenue generating/service impacting systems to I have?
  - How many weeks can I operate for if we're offline?
  - What processes can I not do without?
  - Which 3rd parties do I rely on?
  - Which 3rd parties rely on me?
  - Who do I call if it all goes wrong?

Apply a threat-informed defense



Prioritise treatment by risk:reward

- Over 70%* of breaches involve the human element e.g. stolen credentials
  - What business services do you use that don't support MFA?
  - What passwords do you need to access 3rd party systems?
- Over 80%* of breaches involve a compromised device e.g. a server, an endpoint or a mobile
  - Can employees access your business services from devices they own?
  - Do you work with 3rd parties who rely on contacting you on personal devices?

* Taken from Verizon's DBIR Report, 2023

Principles for working with third parties

- Procurement
  - Be honest with yourself
  - Ensure you have stakeholder support
  - Collaborate with other stakeholders
  - Understand and document your security needs
  - Ask the right questions
  - MFA
- Delivery
  - Be honest with your customers
  - Prioritise investment
  - Engage with the ecosystem
  - Start your improvement programme now
  - Identify capability gaps that, if exploited, may affect your customers
  - MFA

Themes we're seeing

- What are others doing?
  - How are Cisco addressing these changes?
  - How does Cisco's product suite help us address the changes?
- Can you measure our capability and maturity?
- We need to make a once in a generation investment...
  - Segmentation...
  - IR and SOC strategy...

Sample timeline

NIS2 journey

Validate the extent of the journey ahead

Roadmap execution, e.g. implementation of controls, build/enhance response capabilities, education

Compare your security posture against expected regional NIS2 legislation

Jan 2024 | Jun 2024 | Oct 2024

Baseline critical systems, security architecture, controls and capabilities

Operational phase, maturing skills and supporting processes

Emergency Support

Make UK & Europe a hostile place for criminals

(to paraphrase NCSC)

Next steps

- https://www.cisco.com/c/m/en_emea/products/security/nis2-directive.html
  - Engage with internal stakeholders
  - Consider, based on size, investigating Cyber Essentials
  - Review your ISO27001 ISMS if you have one
  - Document your critical assets
  - Contact 3rd parties with whom you have significant business relationships
  - Carry out a table top exercise
  - Engage an Incident Response Partner

Questions?

twadhwab@cisco.com


Cisco
Customer Experience