Grant Thornton

Challenges in Managing Cybersecurity

Christos Makedonas

Partner, Digital Risk

Malta Stock Exchange Governance, Risk and Compliance Summit 2023

02 February 2023

About me

Christos Makedonas
Partner | Digital Risk
Grant Thornton (Cyprus) Ltd

T: +357 22 600 000
E: christos.makedonas@cy.gt.com

- Digital Risk Leader | Grant Thornton Cyprus
- Co-Founder and Director of Enactia GRC SaaS
- Professional Bodies

  Immediate Past President of the ISACA Cyprus Chapter

  Also, member of (ISC)2, EC-Council, CCS, IIA, ACFE

- Cybersecurity Background
  - More than 19 years of professional Cybersecurity experience
  - Advisory, IT Audit, Penetration Testing, Incident Response & Digital Forensics, Data Protection, Compliance
  - BDO, Deloitte, Ex-Laiki Bank, PwC, InfoCredit Group
  - CISA, CIPP/EU, CDPSE, ISO 27001 LI, CCFP, Certified BrainSpace Analyst, CICA, C|EH, E|CSA, L|PT, CFIP, CMI, CSIS

- Academic Background
  - MSc Analysis, Design and Management of Information Systems (ADMIS) London School of Economics and Political Science (LSE)
  - BSc (Hons) Computing Informatics - University of Plymouth – Best Student Price & Professional Membership award from BCS
  - Banking Operations (BO)

Cybersecurity considerations

Cybercrime

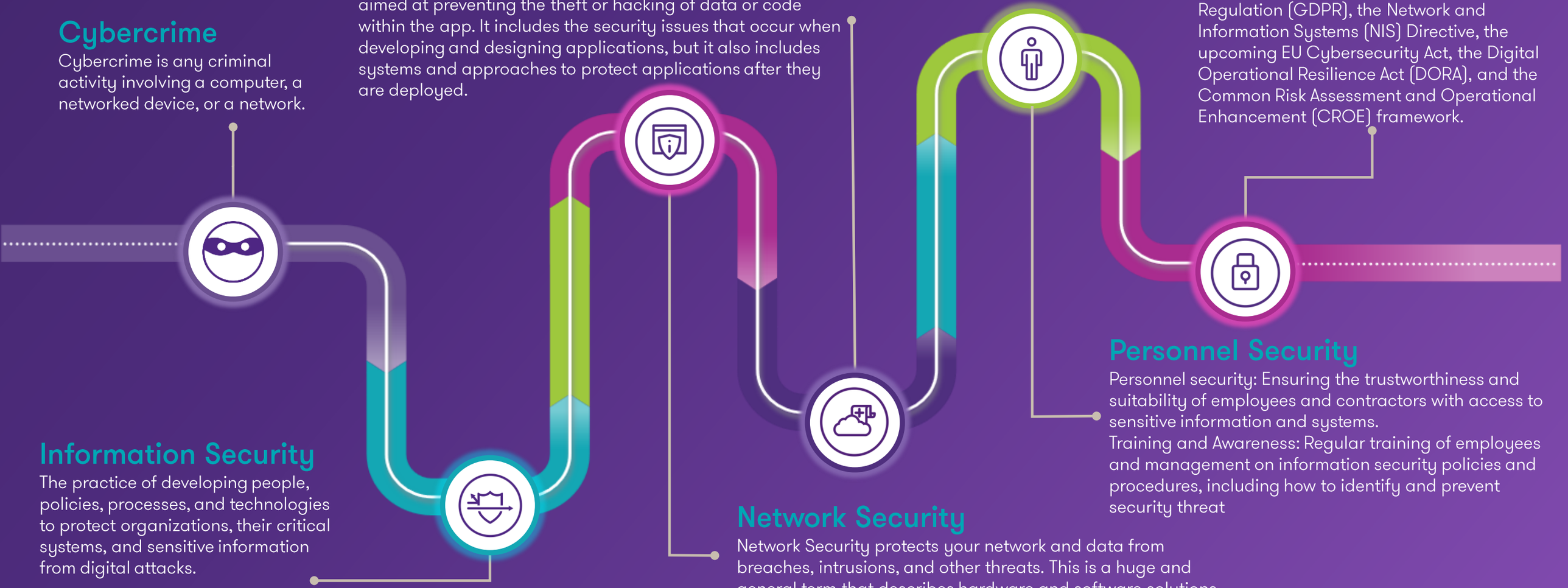
Cybercrime is any criminal activity involving a computer, a networked device, or a network.

Application Security

Application security describes app-level security measures aimed at preventing the theft or hacking of data or code within the app. It includes the security issues that occur when developing and designing applications, but it also includes systems and approaches to protect applications after they are deployed.

Cybersecurity Regulatory Compliance

The EU has implemented several regulations for data protection and cybersecurity, including the General Data Protection Regulation (GDPR), the Network and Information Systems (NIS) Directive, the upcoming EU Cybersecurity Act, the Digital Operational Resilience Act (DORA), and the Common Risk Assessment and Operational Enhancement (CROE) framework.



Information Security

The practice of developing people, policies, processes, and technologies to protect organizations, their critical systems, and sensitive information from digital attacks.

Network Security

Network Security protects your network and data from breaches, intrusions, and other threats. This is a huge and general term that describes hardware and software solutions, as well as processes or rules and configurations related to network usage, accessibility, and overall threat protection.

Personnel Security

Personnel security: Ensuring the trustworthiness and suitability of employees and contractors with access to sensitive information and systems.
Training and Awareness: Regular training of employees and management on information security policies and procedures, including how to identify and prevent security threat

What are the key challenges in managing Cybersecurity?

Challenges in managing Cybersecurity

Keeping up with evolving threats

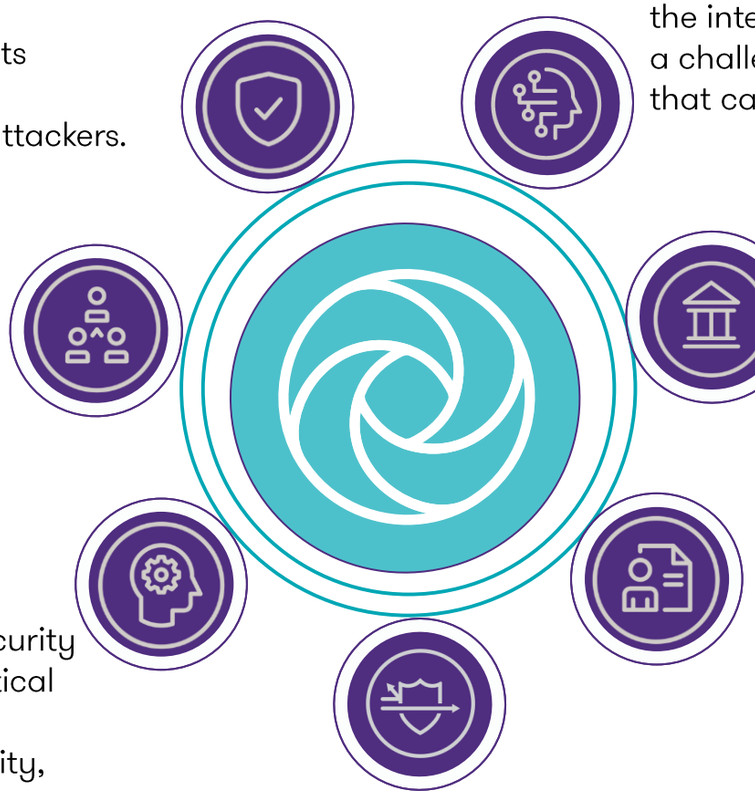
Cyber threats are constantly evolving and becoming more sophisticated. Attack methods such as phishing, ransomware, and advanced persistent threats are increasingly common. Keeping up with these threats requires organizations to invest in security tools, technologies and personnel to stay ahead of the attackers.

Supply-chain / Third-Party risk in cybersecurity

Threats posed by external suppliers, contractors, and partners in an organization's information technology systems and processes.

Human Element

Ensuring that all employees are trained in cybersecurity best practices and aware of potential threats is critical to maintaining the security of an organization. This includes training on topics such as password security, phishing awareness, and safe browsing practices.



Difficulty in identifying and mitigating threats & establishing Incident Response procedures

With the increasing number of devices and networks connected to the internet, identifying and mitigating cybersecurity threats can be a challenge. Organizations need to implement security measures that can detect and respond to threats in real-time.

Maintaining compliance

Organizations must comply with a variety of regulations, frameworks and standards, such as PCI-DSS, GDPR, NIS2, DORA, CROE TIBER, SOC2, ISO27001, NIST etc which can be difficult to manage. They need to understand these regulations and implement the necessary controls and GTC tools to maintain compliance.

Limited resources

Many organizations have limited resources and budget for cybersecurity. This makes it difficult to implement and maintain effective security measures. Organizations need to prioritize their security investments and focus on the most critical areas.

Continual Testing and improvement

Security is not a one-time effort; it is an ongoing process. Regularly testing the security posture of an organization, identifying vulnerabilities and taking steps to address them is crucial to maintaining an effective security network.

Thank you

grantthornton.com.cy