Kiberdrošības kompetenču mērķtiecīga pilnveide

cybersecurity competence improvement

Sintija Deruma, CISM
Banku augstskolas «Kiberdrošības pārvaldība» studiju programmas direktore

- **Vai kiberdraudi ir mīts?**
- **Vai apdraudējumi rada reālus zaudējumus uzņēmumiem?**
- **Vai uzņēmumi ir gatavi kiberkaram?**

Cybersecurity Skills Crisis

Too Many Threats

62% INCREASE IN BREACHES **IN 2013**[1]

1 IN 5 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

US $3 TRILLION TOTAL GLOBAL IMPACT OF **CYBERCRIME**[3]

8 MONTHS IS THE AVERAGE TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION **EXPOSED RECORDS** AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]

Too Few Professionals

62% OF ORGANIZATIONS **HAVE NOT INCREASED SECURITY TRAINING IN 2014**[6]

1 OUT OF 3 SECURITY PROS ARE **NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS**[7]

<2.4% **GRADUATING STUDENTS HOLD COMPUTER SCIENCE DEGREES**[8]

1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]

83% **OF ENTERPRISES** CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

Enterprises are under siege from **a rising volume of cyberattacks.**

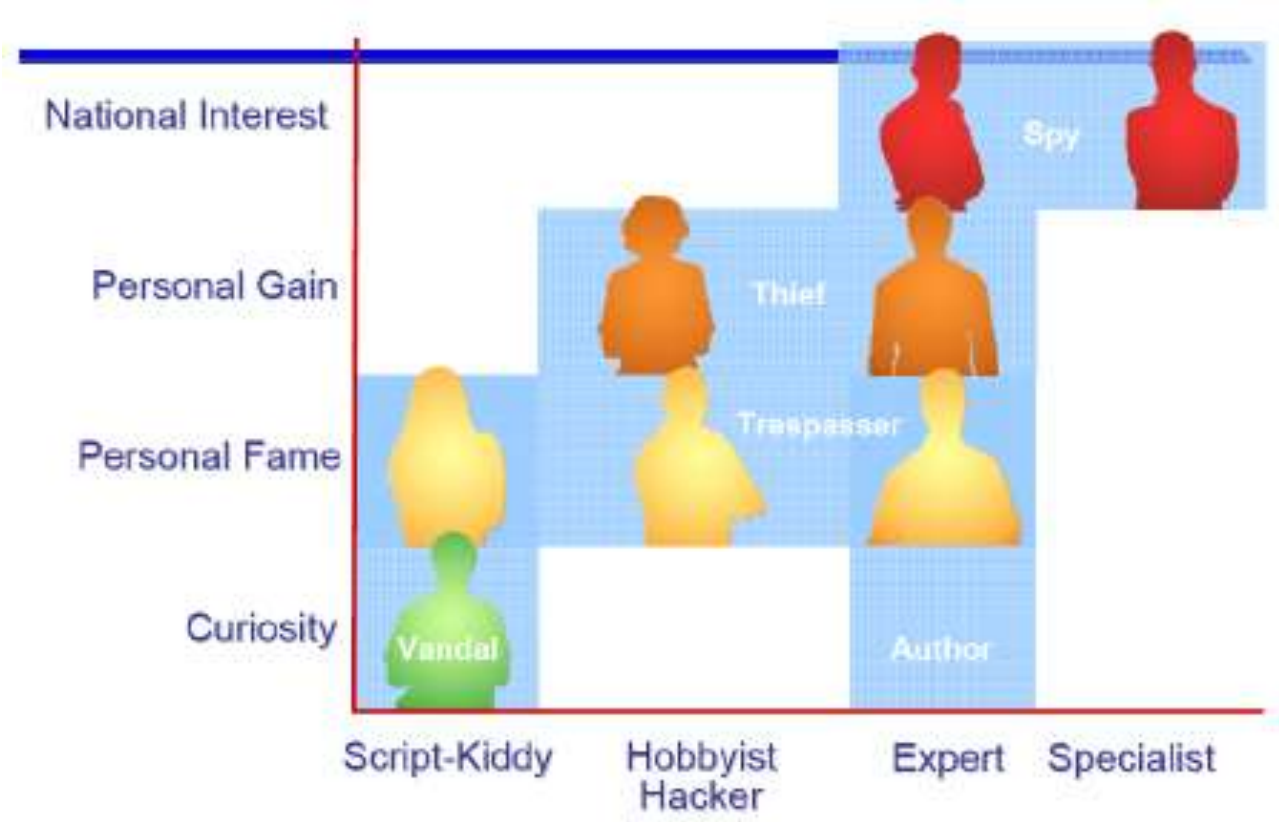
At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **2.** *M-Trends 2013: Attack the Security Gap*, Mandiant, March 2013; **3.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study*, ISACA, April 2014; **5.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **6.** *ISACA's 2014 APT Study*, ISACA, April 2013; **7.** *ISACA's 2014 APT Study*, ISACA, April 2014; **8.** *Code.org*, February 2014; **9.** *2014 Cisco Annual Security Report*; **10.** *Cybersecurity Skills Haves and Have Nots*, ESG, March 2014

CSX CYBERSECURITY NEXUS

ISACA trust in, and value from, information systems

Hakeru klasifikācija



David Aucsmith, 2005

Kas ir kibertelpa?

Kiberdrošība

Kiberdrošība ir instrumentu, politikas, drošības konceptu un vadlīniju, risku vadības, rīcības, apmācības, pieredzes un tehnoloģiju kopums, kuru var izmantot elektroniskās vides, tās organizācijas un lietotāju aktīvu aizsardzībai. Organizācija un lietotāju aktīvi ietver savienotas skaitļošanas tehnoloģijas, personālu, infrastruktūru, programmatūru, pakalpojumus, telekomunikāciju sistēmas un pārsūtītas jeb uzglabātas informācijas kopumu elektroniskajā vidē.[1]

Kibertelpa

Kibertelpa ir interaktīva vide, kura ietver lietotājus, tīklus, skaitļošanas tehnoloģijas, programmatūru, procesus, pārsūtītas jeb uzglabātas informācijas kopumu, lietojumprogrammas, pakalpojumus un sistēmas, kas ir savienotas tieši vai netieši, izmantojot internetu, telekomunikācijas vai datortīklus, un kurā mijiedarbojas tās lietotāji. Kibertelpai nav fizisko robežu.[2]

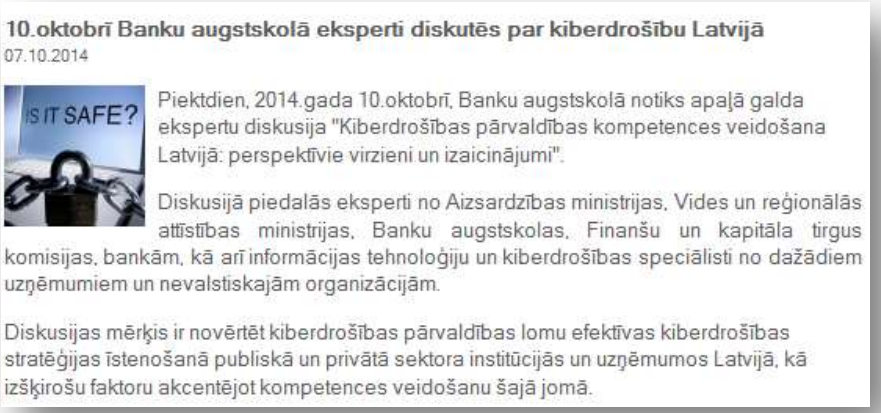
Latvijas kiberdrošības stratēģija 2014–2018

Kāpēc organizē uzbrukumus?

- Informācijas iegūšana vai bojāšana
- Infrastruktūras pārņemšana vai nograušana
- Profesionāļu pārvilināšana vai kompromitēšana

Lai aizsargātu kibertelpu

- Nepieciešama stratēģiska pieeja
  - LV Kiberdrošības stratēģija un rīcības plāns
- Kompetence šo jautājumu risināšanā
- Vienota izpratne par kiberdrošības ekosistēmu



10.oktobrī Banku augstskolā eksperti diskutēs par kiberdrošību Latvijā

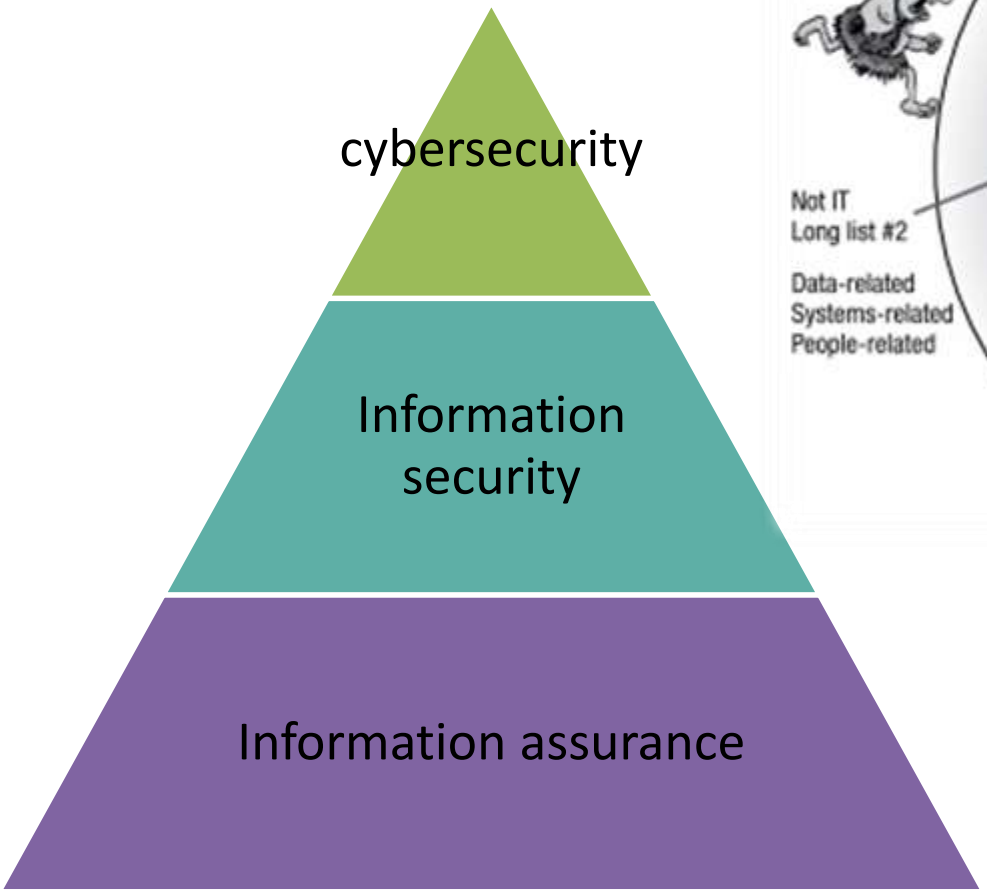
07.10.2014

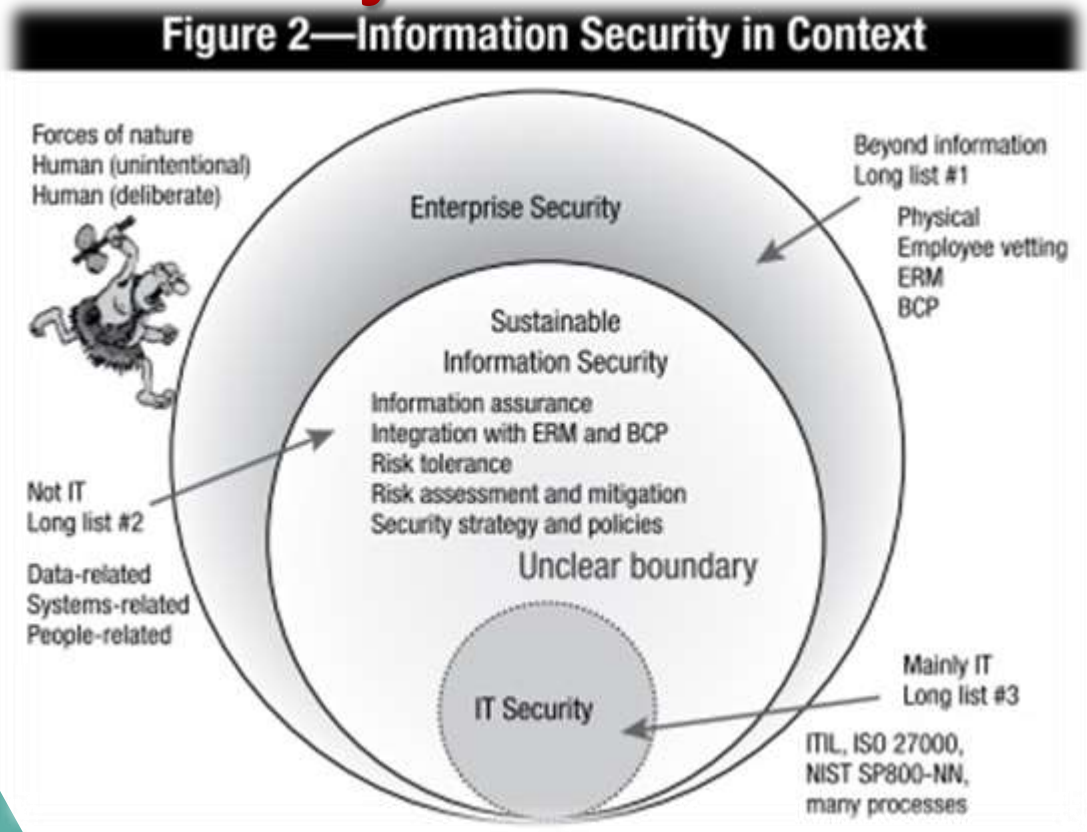
Piektdien, 2014.gada 10.oktobrī, Banku augstskolā notiks apaļā galda ekspertu diskusija "Kiberdrošības pārvaldības kompetences veidošana Latvijā: perspektīvie virzieni un izaicinājumi".

Diskusijā piedalās eksperti no Aizsardzības ministrijas, Vides un reģionālās attīstības ministrijas, Banku augstskolas, Finanšu un kapitāla tirgus komisijas, bankām, kā arī informācijas tehnoloģiju un kiberdrošības speciālisti no dažādiem uzņēmumiem un nevalstiskajām organizācijām.

Diskusijas mērķis ir novērtēt kiberdrošības pārvaldības lomu efektīvas kiberdrošības stratēģijas īstenošanā publiskā un privātā sektora institūcijās un uzņēmumos Latvijā, kā izšķirošu faktoru akcentējot kompetences veidošanu šajā jomā.

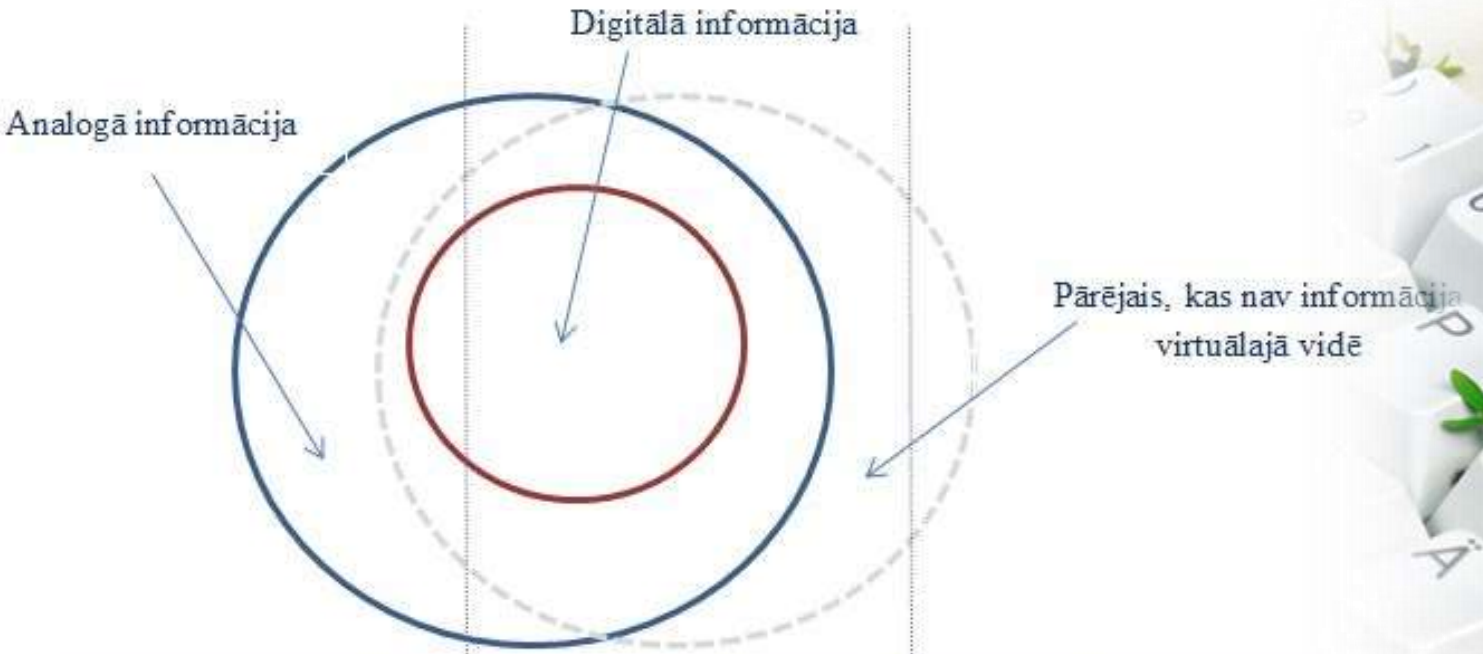
Kiberdrošība ≠ Informācijas drošība





Ed Gelbstein, Ph.D., ISACA, 2012, vol2.

Kiberdrošības ekosistēma



Informācijas drošība	IKT drošība	Kiberdrošība
+ Fiziskās vides D;	+ Datu D;	Informācijas karš
Personāla D;	Tīklu D;	Digitālā revolūcija;
Piegādes ķēdes D	Lietotņu, aplikāciju D;	Lielo datu Cunami
	Programm.kodu D	

D=drošība

Avoti: Aapo Cederberg, Senior Advisor, Emerging Security Challenges Programme, Geneva Centre for Security Policy, 2014 adop. & Mortens Irgens, 2013

Uzticami pakalpojumi

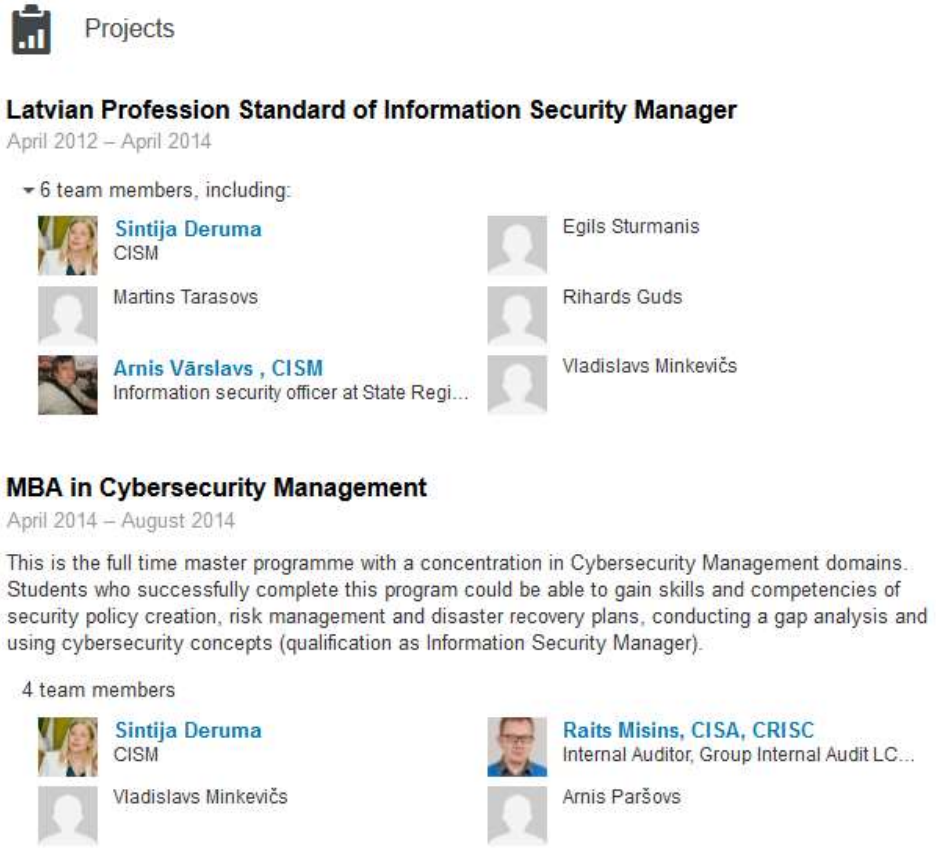
Spēja aizsargāt resursus

Spēja rīkoties krīzes situācijās

Spēja paredzēt nākotni

Jaunās profesijas

1. **Informācijas sistēmu drošības speciālists** 2529 07
2. **Informācijas drošības vadītājs** 1330 09*



** Profesiju kods profesiju klasifikatorā*

Figure 2—Typical Information Security Progression and Management Model

Board of Directors Information Security/Assurance Committee

C-level Cross-functional Team

Career Levels

Level	Management		Technology	Architecture	Assurance	Legal/Risk Management/ Privacy
Senior executive (C-level)	CIO COO		CTO CISO CArO		CAO	GC CRO CPO
Manager/ director	Operations consulting	Development/systems and infrastructure information security			Internal audit	Information risk/privacy consulting
Expert	Principal IT consultant	Senior IT systems professional	Senior IT development engineer	Senior IT architect	Senior information security auditor	Principal IT consultant
Specialist, manager	Product/program/project manager, team leader, account sales manager					
Specialist, technical	Security consultant, business analyst	Security product manager	Security designer	Security systems professional	Security auditor	Information risk consultant
Entrant	Analyst		Developer	Security designer trainee	Security systems trainee	Security auditor trainee

Career movement through the C-level may be vertical, horizontal and/or diagonal.

Source: Adapted from Lynas, David; John Sherwood; "Professionalism in Information Security: A Framework for Competency Development," 12th Annual COSAC Conference, UK, 2005

C-level Key:

CIO = Chief information officer
COO = Chief operating officer
CTO = Chief technology officer
CISO = Chief information security officer
CArO = Chief architecture officer
CAO = Chief assurance officer
GC = General counsel
CRO = Chief risk officer
CPO = Chief privacy officer

Informācijas drošības vadītājs 1330 09*

Informācijas sistēmu drošības speciālists 2529 07

** Profesiju kods profesiju klasifikatorā*

MANAGEMENT	ASSURANCE	TECHNICAL, OPERATIONAL	LAW	RISK, RESPONSE
Chief Information Security Officer	Information Systems Auditor	Computer Systems Security Analyst	Privacy & Security Officer	Incident manager
Information Security Officer	Cyber Warfare & Information Assurance Engineering	Network Security Engineering Application Security Engineering	Data Privacy Officer	Information Security Remediation Specialist
Information Security Manager	Information Assurance Specialist	Forensic expert Penetration tester Cyber Threat Intelligence Analyst		Information Security Awareness Specialist
Security Leader	Privacy & Security Assurance Manager			Risk Officer
Security Strategist	Information Security compliance manager	Technical Security Architect		Information security risk manager
Data Governance manager		Cloud Security Operation Analyst		Business contingency manager
Information Security Consultant		Cyber Security Analyst		Crisis manager
Cybersecurity adviser		Information Security Professional		Security Projects Manager

BANKU AUGSTSKOLA

BA SCHOOL OF
BUSINESS AND FINANCE

Kiberdrošības pārvaldība

profesionālā maģistra studiju programma

Uzņemšana jau no š.g.14.novembra, vairāk www.ba.lv

«Kiberdrošības pārvaldība» profesionālā maģistra studiju programma 2 gadi (pilna laika), 80 KP

1. Cybersecurity &Critical Infrastructure Protection
2. Information Security Risk & Compliance Management
3. Information Security Awareness
4. Information Security Governance
5. Information Security Incident Management
6. ICT Management
7. Leadership
8. Managing Employees, Proffesionals and Projects
9. Security Policy, Leaglislation
10. Cybersecurity Economics

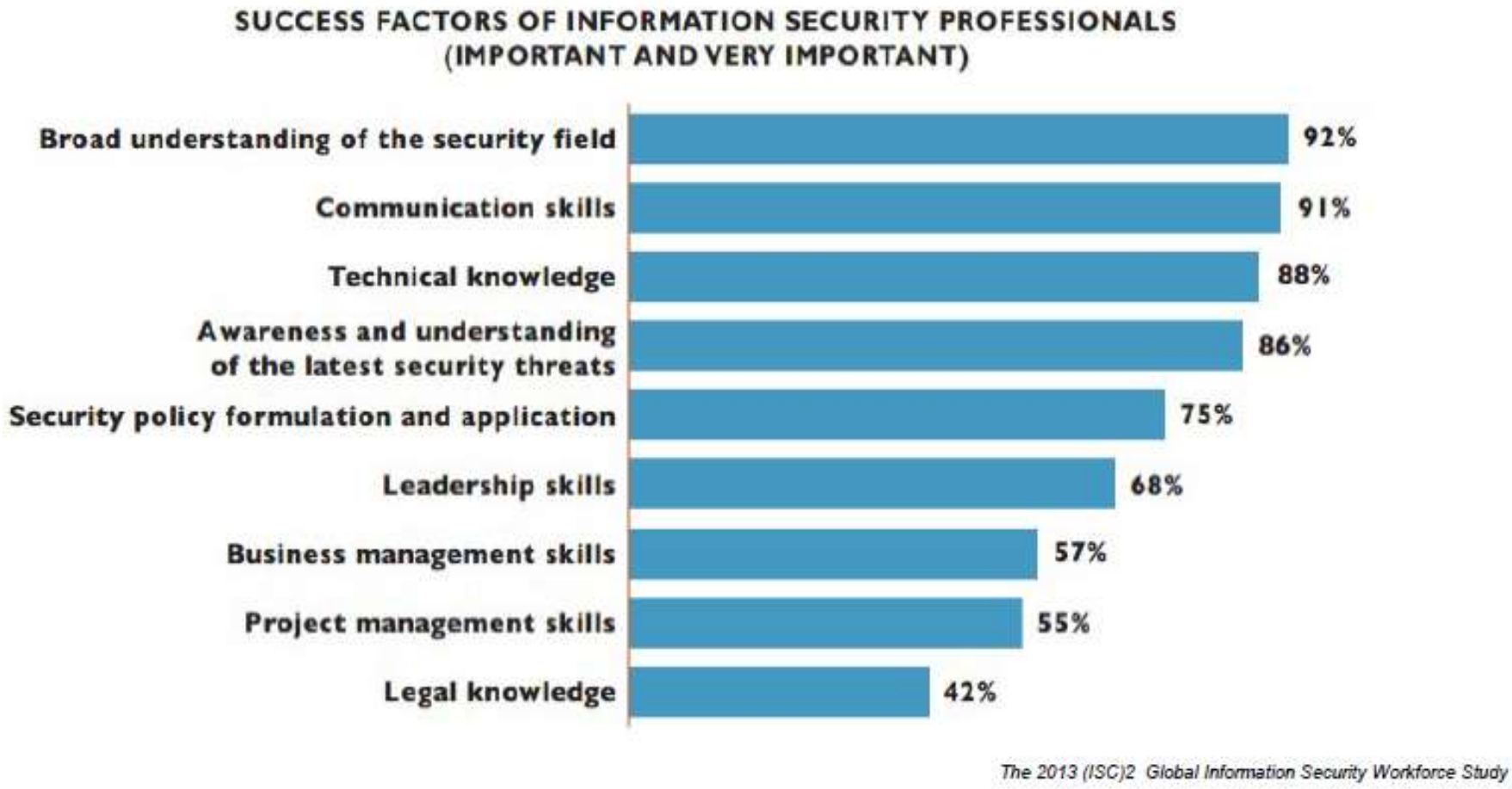
Profesijas standarts 1330 09

CISM zināšanas, prasmes, kompetences

Augstākās izglītības standarts

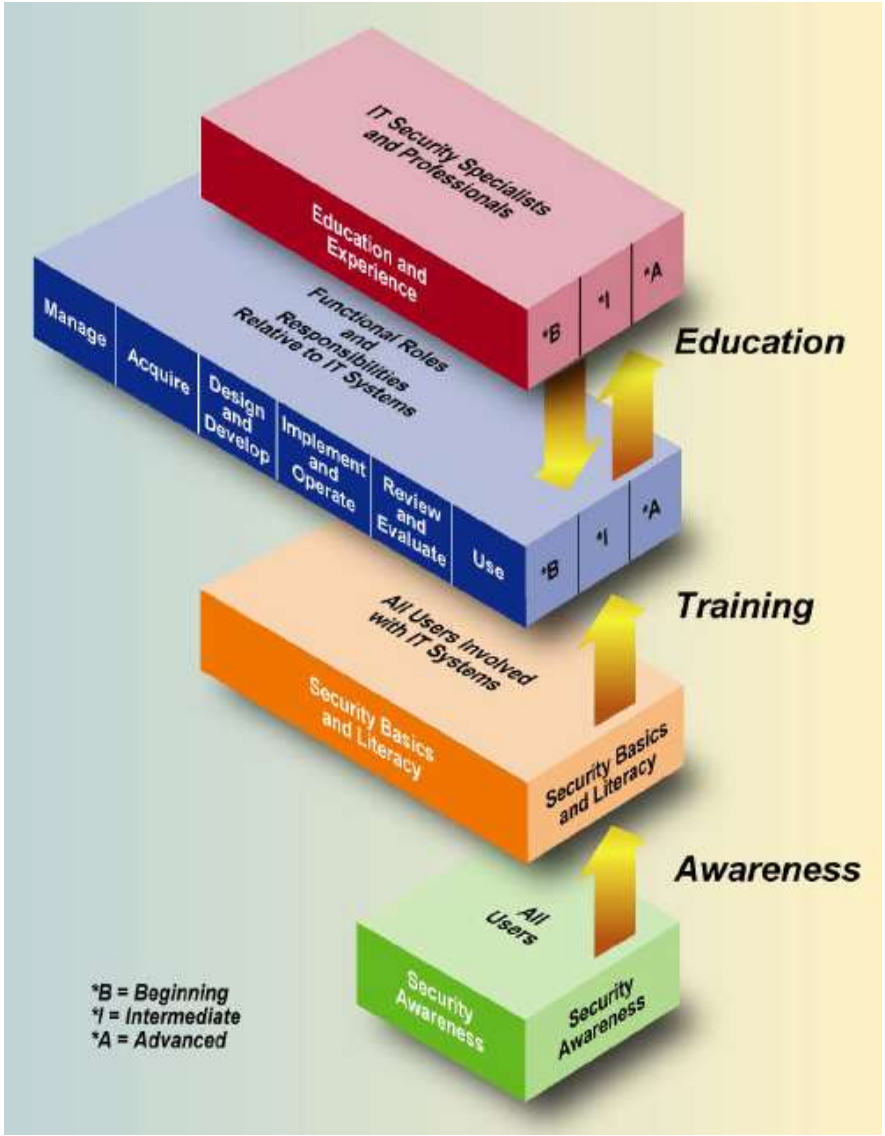
Informācijas drošības vadītāja pienākumi	Uzdevumi
Organizācijas informācijas drošības pārvaldības sistēmas plānošana.	1. Novērtēt organizācijas informācijas resursu aizsardzības vajadzības. 2. Noteikt informācijas drošības pārvaldības stratēģiskos mērķus. 3. Izstrādāt un aktualizēt nepieciešamos iekšējos normatīvos aktus. 4. Ieviest informācijas drošības pārvaldības sistēmas iekļaušanu organizācijas (biznesa) procesos. 5. Nodrošināt organizācijas vadības atbalstu un iesaisti informācijas drošības pārvaldībā. 6. Izstrādāt informācijas drošības pārvaldības sistēmas arhitektūru, noteikt atbildīgo personu lomas un pienākumus. 7. Izstrādāt informācijas drošības pārvaldības kvalitātes vērtēšanas kritērijus un izmērāmos rādītājus. 8. Pārzināt un piemērot IKT nozares normatīvajos aktos noteiktās prasības. 9. Koordinēt informācijas drošības pārvaldības sistēmas atbilstību ārējiem, nozares starptautiskajiem normatīvajiem aktiem.
Informācijas drošības risku pārvaldība.	1. Koordinēt informācijas resursu klasifikācijas izstrādes procesu. 2. Izstrādāt informācijas drošības risku analīzes metodiku. 3. Koordinēt informācijas drošības risku pārvaldības procesu. 4. Organizēt komunikāciju par informācijas drošības riskiem ar visām ieinteresētajām pusēm.
Informācijas drošības pasākumu ieviešana, īstenošana un uzraudzība.	1. Izstrādāt, īstenot un ieviest informācijas drošības pārvaldības īstermiņa un ilgtermiņa plānus, programmas. 2. Informēt un skaidrot organizācijas informācijas drošības pārvaldības mērķus un rezultātus. 3. Izstrādāt un īstenot informācijas drošības izpratnes veicināšanas kampaņas/apmācību programmas, veikt zināšanu novērtēšanu. 4. Nodrošina aktīvu dalību krīzes, ārkārtas situācijas, biznesa nepārtrauktības pārvaldības plānošanā un pasākumu īstenošanā. 5. Koordinēt informācijas drošības pārvaldības izmērāmo rādītāju monitoringu. 6. Izvērtēt, analizēt un sniegt priekšlikumus par informācijas drošības pārvaldības sistēmas efektivitāti.
Informācijas drošības incidentu pārvaldība.	1. Izstrādāt un ieviest informācijas drošības incidentu pārvaldības procesu. 2. Koordinēt informācijas drošības incidentu analīzes un izmeklēšanas procesu.

Veiksmes faktori

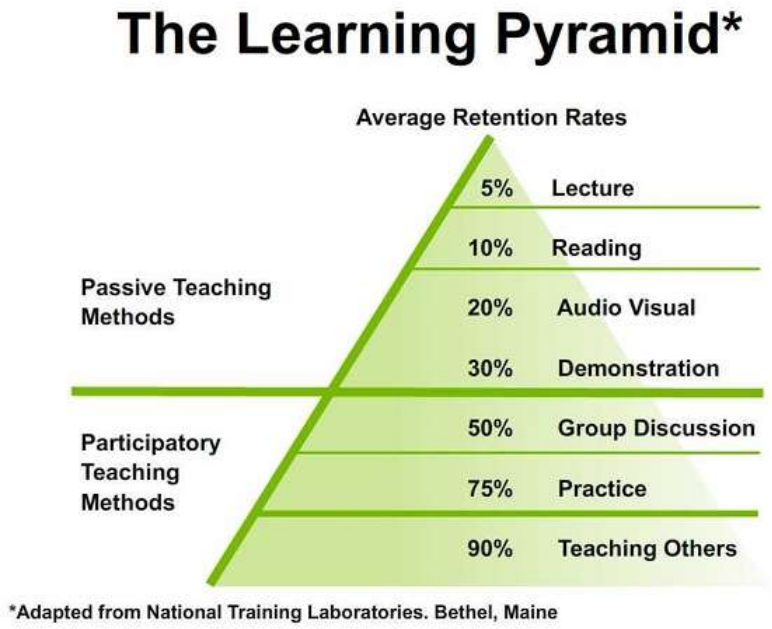


The 2013 (ISC)2 Global Information Security Workforce Study

Izpratne ir labs sākums !



NIST Special Publication 800-50



Piemērs IKT nozarē

"Digitālās darbavietas": vakances un absolventi* (skaits)

* *Pārskati un prognozes, kuros pieņemts mērens IKP un IKT ieguldījumu pieaugums. Šeit ņemti vērā tikai tie absolventi, kas ieguvuši augstāko izglītību IKT jomā.*

Avots: Empirica

teorētiskais IKT vakanču skaits 2015. gadā, būs 864 000…

2012. gadā Empirica, IDC un INSEAD kopīgi veica Eiropas Komisijas Uzņēmējdarbības un rūpniecības ģenerāldirektorāta pasūtītu pētī jumu. Pētī juma "E-prasmes konkurētspējai un inovācijai: redzējums, attīstības plāns un paredzamie scenāriji" mērķis bija izstrādāt redzējumu Eiropas e-prasmju konkurētspējas un inovācijas nodrošināšanai un izpētī t veidus, kā stāti es pretī pašreizējiem un nākotnes izaicinājumiem.

Programmu atbalsta

- LV Kiberdrošības stratēģijā un rīcības plānā noteiktās aktivitātes izglītības virzienā;
- Finanšu industrijas pieprasījums;

- Darba devēju aktīva iesaiste programmas izstrādes laikā: Swedbank, DPA, Cert.lv, AM, VARAM…

Sagaidāmie rezultāti

- Izvēlēties, plānot, ieviest, uzlabot, pilnveidot:
  - organizācijas informācijas drošības pārvaldības sistēmu;
  - informācijas drošības risku pārvaldību;
  - informācijas drošības incidentu pārvaldību.

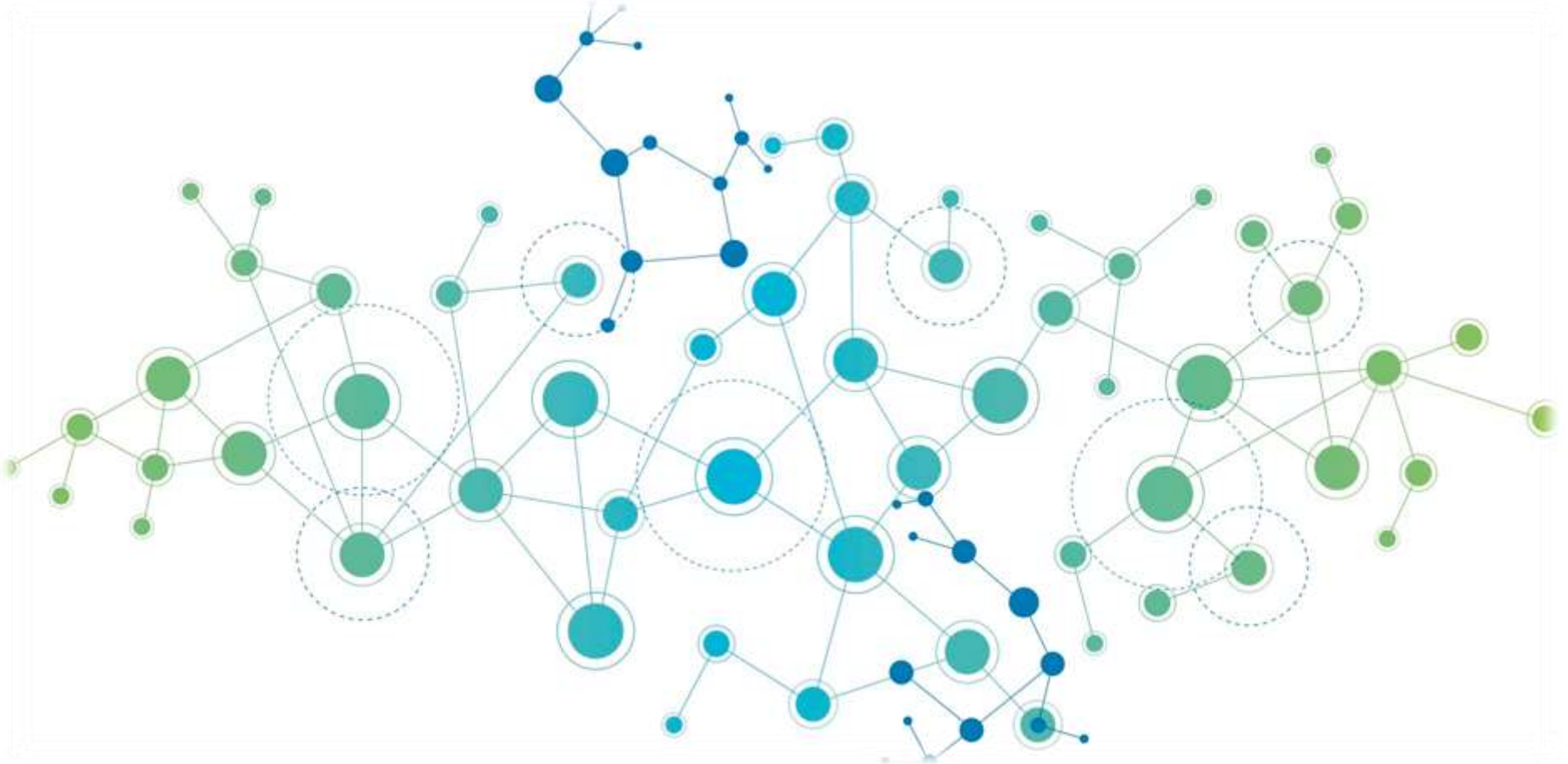
- Izdomāt, izstrādāt, īstenot, piemērot, uzraudzīt:
  - informācijas drošības un kiberdrošības aizsardzības pasākumus;

- Izskaidrot, komunicēt, argumentēt, izglītot, izmērīt:
  - Lietderīgumu, vajadzību, atdevi, ilgtspēju!

Nākotnes plāni

- Attīstīt ciešāku sadarbību ar informācijas drošības, IKT drošības un kiberdrošības industrijām:
  - ISACA
  - LIKTA
  - LATA
  - CERT
- Dalīties ar zināšanām, pētījumu rezultātiem un pieredzi
  - Jau kiberdrošības mēneša ietvaros (ISACA/Cert, DSS konferencēs)
- Izveidot kiberdrošības pārvaldības kompetenču platformu BA.

Paldies!



Sintija.Deruma@ba.lv