Swedish Armed Forces (SwAF)

Effective, Efficient and Secure Information Management
Thesis proposals version 2015-10-01

Contact: Ross Tsagalidis, MSc, Program Manager & POC
Email: wross@tele2.se; **Cellphone:** +46 (0)733-666 982

The thesis is the last major study task for students. Often looking at a government agency or a company, they may gain experience from real projects that provide a good insight into what to expect during an upcoming employment.

• In 2010, The Swedish Armed Forces (SwAF) Defence Staff, Policy, and Plans Department (HKV LEDS INRI) initiated and established a collaboration agreement with the Swedish University community, to enable and augment traditional research and development in the defence sector. Encouraging students to pursue theses and PhD work, improves the Armed Forces' capabilities to exploit knowledge and expertise originating from academia and higher education. The benefits are mutual whereas both universities and students have the opportunity to interact with a dynamic and influential partner in defence and societal security.

• The collaboration covers effective, efficient, and secure information management and is interdisciplinary. Through this partnership the Swedish Armed Forces provides proposals for bachelor and master theses. In the following pages there's a list of over 130 proposals - the students can modify the suggested Topic or propose their own essay Topic. SwAF assigns a subject matter expert (SME) as an associate supervisor. SwAF also provides lectures and seminars for graduate and under-graduate students. In return, SwAF will benefit from novel perspectives on current issues and future operational challenges, from both a methodological, procedural, organizational, legal, and technical point of view.

• The supervision of thesis work requires good management skills, not only of the academic supervisor who is also responsible for the formalities, but also of the SwAF supervisors who are well aware and prepared for this.

You can find information about SwAF at: **www.forsvarsmakten.se**

How you as a student will proceed to get in contact with SwAF for doing your Thesis with us is described in the chart below:

Process description

1. The student selects a Thesis proposal from the List or sends us his/her own proposal.

2. The student contacts the SwAF Program Manager (SwAF-PM), Ross Tsagalidis, or the University Program Coordinator (UPC) for any questions on the Thesis proposals and finally in consensus with the SwAF-PM determines the Topic. The UPC or USV approves it.

3. The UPC appoints a University Supervisor (USV) to the student as his/her scientific supervisor.

4. The USV acts alongside the student according to the University´s internal procedures for the accomplishment of the Thesis.

5. Necessary communication between USV-SwAF-SME, whenever is needed.

6. Collaboration between the student and the SwAF-SME, SwAF Subject Matter Expert, in order to fulfill the requirements for the expected essay outcome.

7. Internal SWAF procedure.

8. Awarding of a certificate after a successful examination.

Note 1: The University Supervisor/Examiner is the one who answers for all formalities as well for the scientific assessment of the content of the Thesis.

Note 2: Personal interviews at SwAF are not for granted. Though any request will be considered and assessed from case to case.

Abbreviations

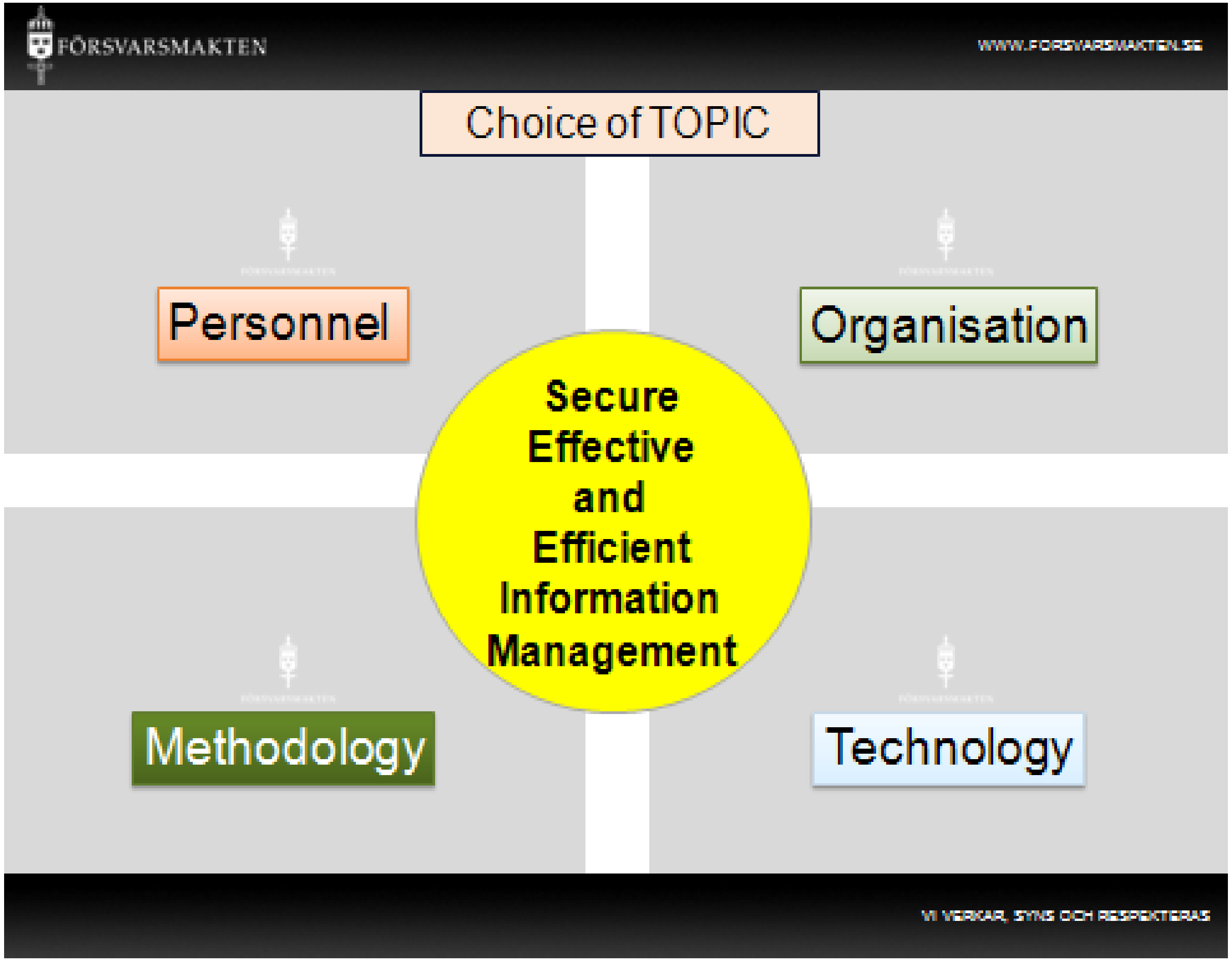
SwAF-SME= Swedish Armed Forces - Subject Matter Expert

SwAF-PM = Swedish Armed Forces - Program Manager

SwAF-S= Swedish Armed Forces – Supervisor

Note: For any query do not hesitate to contact Ross Tsagalidis; wross@tele2.se

A Topic, chosen from the list, can be studied and researched from different angles and perspectives, such as methodological, procedural, organizational, legal and technical.



FÖRSVARSMAKTEN

WWW.FORSVARSMAKTEN.SE

Choice of TOPIC

Personnel

Organisation

Secure
Effective
and
Efficient
Information
Management

Methodology

Technology

VI VERKAR, SYNS OCH RESPEKTERAS

Content of main, and-areas of Theses´ proposals.

CYBER SECURITY (CS)			
CS Management	**CS Threats/Assault**	**CS Defence**	**CS Legislation**
Cyber Defense Exercises, CDE. How to design exercises so that they become a learning experience for the participants? Which logs (Computer, Network, Video, etc.) must be designed to support learning. How to share the results?	Attackers use automated tools to generate thousands daily queries to probe the web for vulnerable web applications. Thesis proposal: A survey of these tools. Categorization in various operational environments and assessment of successfulness	Build and establish a cyber-intelligence and analysis capability for conducting focused operations to detect advanced intrusions, share alerts, and ensure sufficient network services to support mission and operational requirements.	Given that domestic security cannot be separated from international security, where should we set the balance between focusing on our territory and region and engaging threats at a distance?
Leveraging Technology to Ensure Compliance with Cyber Security and Data Privacy Regulations and Threats.	Misuse of "The Cloud": New problems for security people, new opportunities for Cyber criminals.	What contribution should the Armed Forces make in ensuring security and contributing to resilience within Sweden?	How we could more effectively employ the Armed Forces in support of wider efforts to prevent conflict and strengthen the ability of acting.
A balance between technology and methodology managing networks separated deliberately or accidentally and reconnected.	How you tailor innovative analytical techniques to rapidly changing and adapting threats.	Defence against social engineering attacks. A Convergence of Means and Ends for facing cyber threats.	Do our current international defence and security relationships require rebalancing in the longer term?
Can cyber risk insurance coverage hedge your organization's risk stability? If it's feasible is it doable (in terms of business opportunities) for insurance companies?	Electric utilities/SCADA systems must integrate security systems with "proper segmentation, monitoring and redundancies" needed for cyber-threat protection. A methodology to achieve it.	Defence against the latest cyber espionage methods including both insider and outsider attacks. eveloping a Cyber Defense for the IT Assets in a Major Peace and Stability Operation.	Prevention, tracking down and prosecuting cybercrime. What´s possible and what´s doable according to the law?
What sort of information might hackers manipulate for some sort of tactical or strategic effect?	Ransom Trojans take an enterprise´s data as hostage. Countermeasures and solutions.	**See specific Topic for BI in a separate box below at the end of this list!**	

NETWORK/COMMUNICATION/WEB SECURITY (NWS)

Communication Security	Communication Security	WEBB-SEC	WEB-SEC
Developing a Network-security strategy that provides full network visibility and protection for both physical and virtual infrastructure.	How you can control your network if you can't see and touch the physical infrastructure.	Mitigating Data leakage, fraud, identity theft, compromised confidentiality, impaired computing capabilities, legal action, and damaged reputation.	General Methodology discovering system weaknesses and breaches. The system is: work processes, techniques, organization and personnel.
NCS (Network Centric Security). How to achieve this and establish a Common Security Policy for several partners.	Latest DDoS attack and behavioral trends. Approaches to proactive DDoS protection	Web Security Access Control. To exploit the web's potential with complete peace of mind.	Secure Systems Development- A Survey. Is modern IT-systems OS-design less vulnerable than before?
Key distribution in a multilevel system with a single or multi key-servers.	Internet’s Vulnerabilities (known) – a survey. What´s around the corner.	Do Wikis offer a new way to get accurate and updated documents to the armed forces more rapidly?	To exploit the web's potential with complete peace of mind.
How do you protect sensitive, often classified government data from the ever-growing threats of cyber-attacks if the data resides in cloud somewhere? How can you control your network if you can't see and touch the physical infrastructure?	Software Defined Networking (SDN) provides capabilities that go far beyond virtualized L2-L3 switching and routing services. Implemented properly, SDN also enables responsive, automated networks that meet the most challenging application delivery requirements. How one can take the next step toward implementing SDN in the datacenter?	System overload avoidance requires Availability such Mechanisms as Fault Tolerance and Recovery.	WIKI: Create and suggest a Wiki for the Swedish Armed Forces collaboration program with Universities. A source to knowledge as a conceptual model.
Unified Communications & Voice over IP (VOIP). Collaboration, Messaging & Telepresence.	Moving away from a network-centric perspective and concentrating on the endpoints. Pros & Cons	Considerations when evaluating an appropriate DDoS strategy for your organization	

SECURITY MANAGEMENT

Security Management	Security Management	Logging	Security Architect. /Design
The Man-in-the-Browser Attack: Why No One is Safe When Banking Online	Emerging risks from new technologies and social networking. Gain insight for responding to a data breach. Considerations when evaluating an appropriate DDoS strategy for your organization.	**What to log and why:** Establishment of a log management strategy that combines requirements from auditors with a process for the security team based on risk to gain better visibility into log data.	An Information Security model with preventative, evasive and defensive measures.
Who is listening to and intercepting your Calls and Emails? How are they doing it? What can you do to prevent it?			Segregation of duties And, Monitoring integrity.
General security 1. Conduct a catalog with all requirements on security. Everything which is related to security. 2. Categorization of the requirements according to the Info-security tree structure.	Understand how cyber risk insurance coverage hedges your company's risk Why patch management is at heart of an effective security strategy?	Secure Information Management based on user profiles: Which logged data do we need? Trace Agents for active selection due need-to-know, need-to-show criteria.	To get insight into mitigating design and certification risk.
			"Trust" and "Trustworthiness". Prerequisites, criteria and metrics. The ultimate security solution?
Conduct a security plan keeping the red thread, *Quality*, from organisation to personnel, to processes and technology. (Use Miller´s Living Systems Theory)	The importance of a centralized patch and endpoint management platform in mid-sized and enterprise operations.	Quality secured log. Incident description, Incident verification. Normalization/Harmonization of multiple sources.	Organization of a Security Operations Centers (SOC).
Monitor and analyze transmission log. Transmission of log data between different zones	Simulation to test the chosen security solution (what if!)		Simulation to create balanced security.

RISK MANAGEMENT – DATA BASE SECURITY – SOCIAL MEDIA			
Risk Management	**Risk Management**	**Data Base Security**	**Social media**
Methodologies for Information Risk Management, A "market" survey (standards, etc.).	Invent and create a method using *proof due falsification* techniques to ensure that the enterprise´s security policy for its IT systems is protected against man-in-the-middle attacks, phishing/ pharming attacks, key/screen-logger, etc. Defenders vs. Aggressors: A deductive analysis. Defenders vs. Aggressors: An inductive analysis	Conduct a security strategy that identifies user access, monitors database activity, eliminates vulnerabilities, and mitigates risk at the database level.	How do new so called social media have an impact on modern warfare? The failure to engage with audiences across multiple platforms is what is causing problems.
Explain the very real risks to corporate data security and how to assess and grade them.	Risk analysis. How to achieve reliability in risk assessment. (The same threat / vulnerability should result in the same risk assessment regardless of the value)	A simple and cost-effective approach to securing customer account data and hardening up your database ecosystem.	Social media: Something for the Swedish Armed Forces? Social media as alternative communication paths.
Operational risks. Considering collaboration with individuals, groups, organisations.	Risk assessment methods. Standardised or not. A survey and a classification of them.	How to manage data base security in the cloud. Is it better to keep the security management inside or to outsource it?	Social engineering possible due social networking using social media.
Detail the risks to regulatory compliance	To know what to do when early detecting an anomaly or cyber-attack is vital.	A simple and cost-effective approach to securing customer account data and hardening up your database ecosystem. Is the answer PCI DSS?	Social media: Benefits vs costs. Consequences – pros and cons.

ENTERPRISE ARCHITECTURE – IT GOVERNANCE - INTEROPERABILITY

Security/Enterprise (EA) Architecture	GOVERNANCE-RISK-COMPLIANCE	IT Governance	Interoperability
General Methodology discovering system weaknesses and breaches. The system is: work processes, techniques, organization and personnel.	Whether CIOs are managing data in the cloud or managing teleworking personnel, gov-IT operations are increasingly distributed. A governance, risk and compliance, or GRC, strategy can help agencies gain visibility into their programs. Are there any federal standards, policies and mandates to meet?	Is IT governance different from IT management and IT controls? Is it unnecessary if you have already reached compliance with Sarbanes-Oxley (SOX) and other standards?	Operating in Coalition in hostile environment. Key words: Communication, Contingency, Continuity. How to get them work with a minimum of interference and maximum of trust.
How to connect business models with operations via Enterprise Architecture		How to reach IT Governance maturity.	Definitions for the term "information operations (IO)". NATO looks at information operations as a coordinating function. In the United States they look at the technical functions such as network warfare. But fundamentally you don't "do" information operations to people; information ops are a coordinating exercise. A thoroughly review of the terms.
ERP We are talking about to include Big Data. Fast Data, Mobile, Social and the Cloud. Can elder ERP systems handle those promising factors?		IT governance standards are too expensive to implement. False or True? Are the benefits that can be achieved by following the best practices should outweigh these perceived issues	
How Enterprise Architecture could be the base for a migration into the cloud.	To get insight into mitigating design and certification risk. Segregation of duties And Monitoring integrity.	**ISO/IEC 38500** is an international standard for Corporate governance of information technology. What's the benefit or disadvantage in comparison to COBIT, ITIL?	
Organization of a Security Operations Centre (SOC).	An Information Security model with preventative, evasive and defensive measures.	Simulation to create balanced security. Simulation to test the chosen security solution (what if?). Describe models of Information Security models.	How to raise your security game in an evolving virtual world.

INFORMATION MANAGEMENT

Information Assessment	Information Quality/Assurance	Information Management (1) Share Point	Information Management (2)	Information Management (3)	Communication between security domains
Categorization of information types. • Private • Government • Others Releasable to: • Need to know • Need to see A methodology.	Info-overflow. ”Weight” the amount of meta-data surrounding an object at the, a) Sender b) Receiver	Metadata from a security perspective. Risks and benefits! Solutions for metadata tagging. – Conduct an overview.	Remote central admin of IT-systems vs. Distributed. The impact and the prognosis of consequences on users considering roles, delegation, traceability and the overall automatic distribution of user privileges.	Help CIO's/IT managers understand how patch management fits into the modern security equation.	General Methodology discovering system weaknesses and breaches. The system is: work processes, techniques, organization and personnel. Simulation to create balanced security. Simulation to test the chosen security solution (what if?)
Tools for rational Information Management.	How to measure and manage psycho-social impact on assessment of information.	SharePoint as document and archive system. Strengths and weaknesses. (Constraints)?		Methodologies for the creation of Rational Info-Management. (Automated, Manual, Paper, Digital, Verbal)	
Criteria for comparing information assessment. Controlled Unclassified Information	To trust incoming information. How to verify data integrity.	Alternatives to SAP as ERP-system for governmental authorities. Strengths and weaknesses.	Possibilities and limitations of the Dublin Core metadata standard	How to deal with different metadata taxonomies in a company or agency? Method/process for creating taxonomies of folksonomies	Situational and Domain Awareness
					Information Exchange Gateways, IEGs, a market overview.

CLOUD COMPUTING - VIRTUALISATION

Cloud Computing	Cloud Computing	Cloud Computing	Virtualization	Virtualization
Capturing data automatically and storing it offsite in data centers. Risks and opportunities globally, regionally and locally. Outsourcing: Risks and opportunities	Anti-malware management from the cloud. Anti-malware solutions for servers and desktops that support Mngt tools/reports. The provision of an environment that makes the desktops obtain anti-malware updates across the Internet and make management/exception reports available. Providing services to supply the updates and provide reports.	How to make a cloud computing environment – whether it is a private, public or hybrid 'community' cloud - more secure so that it conforms to very high security and network resiliency requirements.	Successful cloud deployments. Revealing best practices and strategies for how organizations should migrate sensitive data to the cloud, while establishing and sustaining the requisite levels of security, privacy and trust.	Services in the Cloud: Software-as-a-Service (SaaS), PaaS, IaaS, etc. Feasible within Swedish Armed Forces? A way to go and how!
Public, Private and Hybrid clouds. Pros & Cons.	How to raise/ensure your security level in an evolving virtual world	Public, Private and Hybrid clouds. Pros & Cons.	Next generation data centers and the realities of virtualization of security management.	Virtualization a better way to effective and efficient information management.
Cloud Computing – Managerial Concerns: What´s in it for the organization and a market survey. Actors and solutions.	How cloud computing can be a tool that enables the Swedish Armed Forces to manage, monitor and secure the information flowing through its network.	The security strategies needed to defend a virtual environment The security solutions needed to defend your virtual platform	Server virtualization speeds up server replication and deployment, which increases configuration management security challenges. True or false?	Virtualized security. Virtualization and MLS. A solution for better security. Pros & Cons.
Database Security Management in the cloud	Working in the Cloud: Management, Financial and Legal aspects.	Outsourcing: Risks and opportunities	Green IT & Operational Compliance	Virtualization, Storage & Datacentre Optimizations

MAN-MAN/MAN-MACHINE/MACHINE-MACHINE INTERACTION

			Social Engineering
How to create organizational superiority due human intelligence for immediate response.	IT risks are prioritized by their potential impact on the operations. A methodology of risk classification.	Information Reciprocity in multilateral co-operational networks. Conditions and Common accepted requirements building trust.	Social engineering based on public sources.
EA (Enterprise Architecture). What, Where, When, Why, Who, For Whom.	How to create organizational superiority due human intelligence for immediate response?	Biometrics (all in Pros & Cons Propagation	
Effectiveness metrics - Methodology		Using standard components as sensors, to detect zero-day-attacks.	
Model/s for rational IM and Survey of Document Management Applications.			

INTERNET of THINGS (IoT)

Security	Privacy	BYOD	Mobility	
Security mechanisms and protocols defined	Privacy aware data processing User centric context aware privacy and privacy policies	Minimization of portable devices at work. What are the needs and where in the organization makes the decision who will use what?	A wireless device to demonstrate low probability of intercept, low probability of exploitation and low probability of detection.	.What to design to provide CIOs and business leaders with a better understanding of how mobility technology-driven changes in the workplace demand changes of the role of IT and the way in which technology innovation is managed in the enterprise. I.e. - Enterprise Managed Mobility? - Mobile Application Management and Development? - Enterprise Social Networking? - Enterprise Collaboration?
The multi connectivity of the devices sounds great! But this multi connectivity is the weakest point for IoT devices. If one device gets hacked into, the hacker can use it to control all the other devices and retrieve sensitive information like bank credentials and passwords. - What are the options to avoid the consequences?	Security and privacy profiles selection based on security and privacy needs	USB/portable devices have evolved into useful storage media, but they've also turned into a security nightmare for organizations. Security Solutions	Drown essential mobile data security strategy. How to protect and secure mobile end point security weaknesses.	
Virtualization and anonymization	Privacy needs automatic evaluation	Portable devices: Threats. Risks, vulnerabilities, solutions. Protection measures.	Security solutions that can protect your mobile devices, as well as assist you in managing incidents remotely.	
Context centric security Self-adaptive security mechanisms and protocols		Administration of the mobile workforce and in particular, the mobile endpoint security issue.	How pervasive wireless creates new security risks. Strategies you can take to counter the issue.	

BUSINESS INTELLIGENCE (BI) – FINANCE IMPACT

Market analysis	BI		Financial impact
Identify, assess, and mitigate IT risk: A market survey of latest techniques. Pros and Cons.	Business Intelligence. Adequate information is the basis for good decision making. Without techniques to analyze it the information could become worthless (or at least of little value). What is adequate information regarding (cyber-) security?	Shut-off mechanism. The Armed forces could save around 30 million kWh/year by completely turn off computers not in use. Develop mechanisms that, in a controlled manner, automatically turn off idle computers (computers with inactive users). The control system can be directed to apply within or outside the time intervals.	Survey: Models and standards for assessing risks in general regardless operational environment, i.e. Financial, Industry, Public sector, etc.
Market Survey: **A look at the secure data transfer solutions in the marketplace today.**			Merging needs like Economy, Effective and fast Technology - fewer connecting points and availability.
Freeware vs. Licensed Antivirus, Emerging Antivirus Technologies, etc.	Business intelligence as an "umbrella" term to describe concepts and methods to improve business decision in Information Security making by using fact-based support systems.	Convert security data to information and present it appropriately to C level management.	Assessing the True Financial Impact of the "Cloud" – Private, Public, Hybrid, and Community Cloud.
A market survey: Processes and technologies that support information security management (ISM) operations?	To provide Security professionals with BI self-service tools for effective and efficient incident analysis facts.	Develop methods to detect / quantify the value of business intelligence. This in order to be able to make the right trade-offs in the choice between the insulation to reduce the risk of information loss, and thus losing the ability to draw conclusions relating to information.	Assessing the True Financial Impact of Cyber Risks
See specific Topic for BI in a separate box below.	Enforce access to policy data using BI for enhanced security awareness.		Explain the costs vs. benefits to regulatory compliance from an economic perspective.

IDENTIFICATION & AUTHENTICATION Mngt, Access Control

Damaged data retrieval. Examine and suggest mechanisms. Examine and suggest UPS mechanisms/solutions regardless data system environments.	IAM Federation and Automated Account shift & Privilege PKI in federated cloud and mobile security.	The Architecture and the Design of an end-to-end Identity Management Solution.	Define and establish roles and ownership structure considering different levels of information stages (creation, sharing, dissemination, modifying, archiving and retrieval).
Password Management. How to deal with the necessary iniquity.	Classification and authorization in a multirole user environment.	Anonymization advantages for personal integrity included secure identification and authentication of the user.	Satisfactory/Sufficient Security: Used of attribute/criterion. A declaration to tiering - A value table.
Rational Data Retention structured logically.	Delegation and Distribution of user Privileges.	Conduct strategies that are required for the efficient, secure and compliant management of passwords.	How deploying two-factor authentication allows you to confidently establish a person's identity when providing access to sensitive data, networks, or applications.
	Models for secure Information Management. Mitigating Design and Verification Risk Through a Robust Test Environment.		Role Based Access Control (RBAC) – Rule breaking when emergency situations appear. Role takeover in a controlled and not pre-programed way.

POLICIES – AWARENESS - COGNITION

TRUST	SLA/Data media/ UPS (Uninterruptable Power Supply)	Awareness	Regulatory
	UPS, the art of survival. A survey of existing products, solutions and tools for keeping continuity with your operations.	Create an interactive verbal tutorial to provide security instructions in the office and at the field. Use of Artificial Intelligence/Chatbots!	Situational and Domain Awareness. A methodology to achieve it.
What's about trust! New digital trends surface daily, and you've got countless shiny objects clamoring for your attention. You need to know which technologies will deliver the best possible experience for your customers, in your unique context. How to get a measured approach. Your research cuts through the hype and shows which technologies are emerging, overhyped, and really ready for prime time so that one can understand which trends and technologies to use – and which to avoid.	Help CIO's/IT managers understand how patch management fits into the modern security equation.	To be a contemporary user of all new and future social media applications; at the same time a well aware and informed user knowledgeable to handle them with great sense of security.	Educate on solutions preventing unauthorized and/or ex-employees from accessing sensitive and/or valuable company information
	SLA, whip or carrot? A comprehensive SLA procedure within and between agencies.	Early warning messaging systems. Dissemination of alerts and handling instructions throughout the whole organisation.	How can you capture empirical experience in information security, document and circulate it?
		Using Chatbots for Security Training.	An effective information security program. What's the key – if any - providing a complete security solution?
		How to influence the human factor to mitigate the spread of malicious code.	

PRIVACY & INTEGRITY

Identification	Law enforcement		
Stylometry – the study of someone’s unique style of writing – can be used to identify anonymous posters in online forums.Stylometric analysis could also become a common tool for law enforcement and government agencies to uncover supposedly anonymous posters on web forums, although this technique requires a large amount of data to be effective.	Malware is now being used in criminal investigations by remotely inserting tracking technology into mobile phones and following suspects with geolocation technology remotely installed. It’s also used to infect suspects’ machines directly. The pros and cons.	Building privacy from the ground up. When done right, building privacy into a product starts on day one and is thought about at each and every stage of development. The protection of user privacy builds trust and loyalty.	**The Biggest Risk to Privacy Online?** Plaintext data. Data breaches and security failures are a part of online life. Encrypting data from end to end so that 3rd party services who store your data never have plaintext access leaves privacy as the best form of security.
There's also "device fingerprinting," a technique that allows them to recognize you via your browser settings. While this approach was originally invented to fight online fraud, the ad networks have co-opted it, just as they did with cookies in the 1990s.	Most of us view personalization and privacy as desirable things, and we understand that enjoying more of one means giving up some of the other. This tradeoff has always been part of our lives as consumers and citizens. But now, thanks to the Net, we're losing our ability to understand and control those tradeoffs."	As we noted in our first explainer, privacy is a personal choice and different people are going to have different interpretations about what represents a violation of their privacy.	

THREAT & SECURITY INTELLIGENCE _ CRITICAL INFRASTRUCTURE			
Identification			
Security Intelligence - What it Really Means and How to do it Effectively in Your Business **60% of breached organisations included in the 2015 Verizon DBIR were initially compromised within minutes, and yet for most of those organisations it took hundreds of days to detect the intruders.** With that, the Information Security world has embraced the world of intelligence to help detect and respond to modern cyber threats. Discover what Security Intelligence really means in this context, and how it can be performed effectively in an organisation to enable better and faster self-detection of threats, resulting in faster response times and a reduction of total risk		Addressing critical national infrastructural issues, such as the energy sector key points including security of supply.	Threat intelligence may be one of the most over-hyped capabilities within information security because depending on whom you ask you are always going to get a different answer. Every security vendor markets and espouses the virtues of their approach to actionable intelligence, but what is most important is security and risk leaders figuring out a way to differentiate and dedicate their limited resources to the most beneficial intelligence. **Thesis´ topic:** Figure out the key characteristic of actionable threat intelligence and suggest how to maximize threat intelligence to protect your digital business from targeted cyber-attacks

AUTOMATION

How to establish and implement automated capabilities for these key areas:

1. *Access control*
2. *Segregation of duties*
3. *Security incident procedures*
4. *Policy monitoring and enforcement*
5. *Security system planning*
6. *System testing and evaluation*
7. *Assessing, monitoring, and alerting on vulnerabilities in real-time*
8. *Remediating vulnerabilities and security incidents*

SHARE POINT

- Build Information Architecture for SharePoint Document and Records Management.

- Planning the management of corporate information: what goes where between SharePoint, data applications, intranet, shared drives, EDRM, email accounts, paper and Enterprise 2.0.
- Information governance issues. Different types of SharePoint sites. How to use the Records Centre.

- Conducting an Information Audit: objectives, options and outputs. Direct and devolved methods.
- Creating a classification scheme and applying it to the SharePoint site structure. Mapping the Information Audit to the scheme. Design constraints, principles and tips.
- Access control. Designing retention schedules. How to apply them to your SharePoint sites.
- SharePoint as ECM (Enterprise Content Management) -system. Strengths and weaknesses.

BUSINESS INTELLIGENCE

The world of business is becoming increasingly digital. It is enabled by Mobility, Cloud, Big Data and Social. Formerly successful business models are disrupted while on the other hand there are major opportunities. Companies need to understand implications and be prepared.

At the same time, the customer experience is evolving rapidly, with applications and service now key to the whole sales process and after-sales support. In the midst of this, the IT department is being pulled in many different directions. They need to support both the existing technology needs while also looking to enable innovation to keep the company competitive. Agility and flexibility are key aims.

Research questions:
What you will need to think about from technology, people and process to achieve your goals.
How to support the digital enterprise by simplifying, automating and securing your Data Centre.

CYBER SECURITY

1. Bolstering Cyber Defenses

Agencies need a proactive and consistent approach to ensure the confidentiality, integrity and availability of information assets. Continuous Diagnostics and Mitigation could provide the essential toolset to combat increasing cyber attacks, protect sensitive information and mitigate security breaches. How can you help agencies comply with multiple regulations, directives and standards? Create/innovate a toolset for diagnosis and mitigation of security breaches.

Research questions:

- How to achieve real-time asset discovery and risk assessment?
- What are the benefits of automated, context-driven response and remediation?

- How can existing information security systems to strengthen cyber defense be linked and compliant to a certain regulation?

2. Defending Against The Security Threat Within

Rogue nations, hackers and organized crime are the cyber villains that everybody loves to hate...
But in a 2014 survey, the most-cited cause of data theft was employees.
Yet employees are not the only source of insider threats. Trusted third parties with access to networks and data, including current and former service providers, consultants and contractors are also major sources of data theft.

Data Theft Prevention (DTP) is the proactive approach to defending your critical data against both internal and external threats. It coordinates technology, processes and policies to optimize visibility and control of your data, regardless of where it lives or how it's used.

Research questions:

- Are existing DTP technologies reliable and efficient?
- Are existing DTP technologies alone enough to protect an organisation against Data Theft?

3. How would you react to a cyber-attack?

Published *Data Breach Investigations Reports*, tell you that attacks happen fast, and they're more complex than ever – so it's a struggle to keep pace. But understanding the threats an organization is facing and responding swiftly when faced with an attack are two very different things. It takes a strong plan, backed by experts at the ready when every minute counts.

This requires a response plan!
A well-established Response Plan puts an incident response and forensics team on call 24x7, so the organisation can respond to threats quicker. Experts on the case by phone and an on-site investigator en route to your premises in as little as immediately. A dedicated investigative liaison could be a partner to lead response efforts and begin working to pinpoint the source of the suspect activity—and then take steps to help you contain it.

INTERNET of THINGS (IoT)

Scale and Secure the Internet of Things (IoT) with Intelligent DNS Services.
You’ve heard industry projections for 50 billion connected devices worldwide by 2020. It's these devices that will transmit and receive far more data than the Internet has ever seen! To ensure continued fast and reliable connectivity, service providers need to massively scale their networks to handle not just applications and videos, but also the explosive increase in data and network signaling traffic. The key is flexibility and extensibility in network design combined with increased security and network intelligence. Together with the growing IPv6 deployments, it is now more critical than ever for operators to hyperscale and secure DNS traffic.

How can you cover the end to end connectivity and processing of IoT data, and delivering data from the device to the platform while ensuring resiliency, stability and the ability to scale no matter what the demand? From street light to smart car, you need to scale for billions of end points connected to a dependable platform, and getting the balance right between public access and private control is key. How can you achieve end point scaling and data processing on a global scale?

How can you,

- Respond to the surge in DNS queries that may impact network availability?
- Mitigate potentially damaging effects from Denial of Service attacks against DNS?
- Optimise subscriber quality of service based on network and application health and availability?
- Connect IoT devices over public and private networks?
- Establish public level access, private level security?
- Build a global IoT platform?
- Collect data on a global scale?

INTERNET of THINGS (IoT)

Control and management of sensitive IoT data

What is needed to achieve the following goals?

- Data protection – The data must be kept available and safeguarded. This requires full recoverability and the ability to mask or encrypt data, depending on user class.
- Data governance – Regardless of where the data has been sourced, once the data resides in the data lake, the enterprise becomes fully accountable for its provenance and use. It must carefully track the lineage of data as the initial building block for preserving auditability.
- Security – As a source of enterprise data, your solution must manage access control and authorizations.
- Performance and high availability – Like any enterprise data platform that supports mission-critical processes, your solution must meet SLAs and deliver reliable availability.
- Manageability – Like any enterprise data platform, management of operation should be fully automated and highly visible down to node level. Policy-based disaster recovery becomes a must.