Proactive Counter Espionage as a Part of Business Continuity and Resiliency

Lydia Kostopoulos, PhD

November 2015

Summary

Traditional cyber security defenses center around technology, with controls around networks, servers, devices, software as well as data. This approach helps mitigate technological threats but not human based threats. This paper proposes a proactive counter-espionage plan that acts as an additional layer of protection with a human-centric focus adding rigor to technology-centric defense in depth approaches.

The strategy which is presented in the form of a scalable roadmap discusses the means in which information assets and business continuity is protected, importance of operational security audits, reverse open source intelligence and classification of employees who are prime targets for disruptive espionage.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented and is above party politics.

The increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, brings with it major opportunities but also risks: thus, decision-makers in the private sector and in politics depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, economy, international relations, and security/defense. ISPSW network experts have worked – in some cases for several decades – in executive positions and thus dispose over wide–ranging experience in their respective fields of expertise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

Espionage in Ancient History

While cyberspace is new to human history, espionage is not. In fact it has been a strategy that has helped empires gain strategic advantage, flourish and dominate continents. One such example is the Silk Road, not the 21st Century black market SilkRoad website selling illegal goods[1] but the original 1st Century Silk Road trading route which stretched from the Chinese Empire through to the Roman Empire. At the time China had a monopoly over the silk market and traded with the rest of the world, while guarding its secret silk tradecraft. Six centuries later their silk monopoly was going strong, and they had no idea that it was about to be shattered by the end of the century from an empire on the other side of the world. Tired of having to rely on China for the highly in demand and expensive silk to arrive to his Empire and being at the whims of the Persian Empire to have it pass through, the Byzantine Emperor Justinian tasked two monks to go to China learn the silk production tradecraft and smuggle the silkworm eggs out of China through the Silk Road and back into Byzantium.[2] The two monks spent time in China discretely observing and committing to memory the tradecraft of raising silkworms and the silk production. Once all the needed information was acquired they smuggled silk eggs into bamboo canes and made their journey back to the Byzantine Empire. As a result Byzantium became the silk monopoly for the continent of Europe, the Chinese silk monopoly was destroyed and the economic foundation for the Byzantine economy was paved for its remaining 650 years reign.[3]

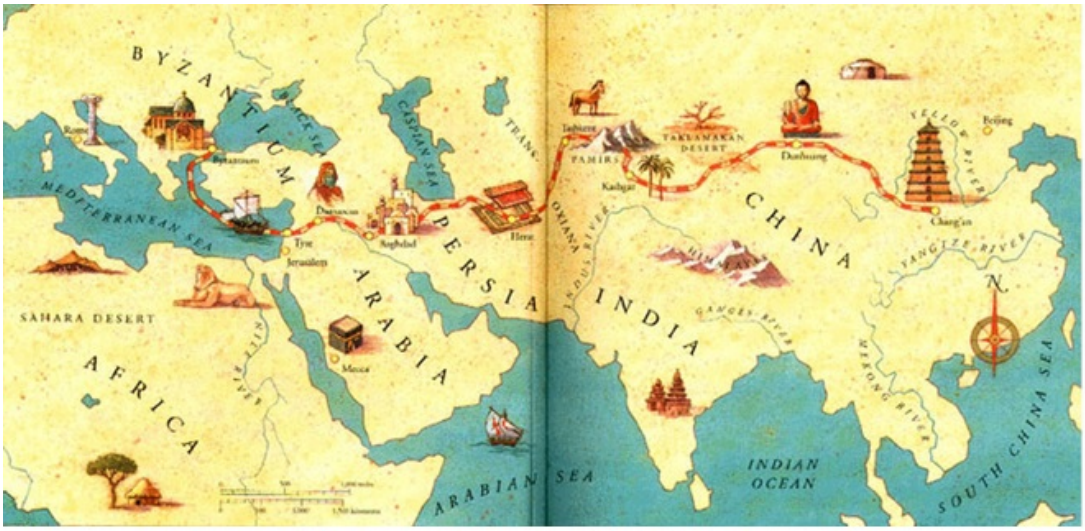


Image source: http://apworldhistory2012-2013.weebly.com/uploads/9/9/9/6/9996001/8757598.jpg?696

Highly in demand trade secrets provided the Byzantine Empire power, money and advantage. Fifteen centuries later, countries with state of the art trade secrets that are highly in demand continue to be able to exert power

[1] Burleigh, N. (2015). "The Rise and Fall of Silk Road, the Dark Web's Amazon". Newsweek. http://www.newsweek.com/2015/02/27/silk-road-hell-307732.html
[2] Mark, J. (2014). "Silk Road". Ancient History Encyclopedia. http://www.ancient.eu/Silk_Road/
[3] University of Washington. (2015). "Silk Road Art". http://depts.washington.edu/silkroad/exhibit/trade/silkae.html

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

more than those who do not, their economies continue to be more conducive to greater technological improvements, and these countries continue to have a competitive advantage over countries who were not able to develop because they lacked the coveted highly in demand trade secrets.

Despite many having said that the human is the weakest link in information security, human defenses are not as rigorously set up as technical defenses. According to Trend Micro, 91% of cyber-attacks begin with a spear phishing email. [4] Although 156 million phishing emails are sent every day, only 16 million make it through the filters; however even then 800,000 links are clicked and out of those 80,000 people disclose confidential information after having clicked the link. [5]

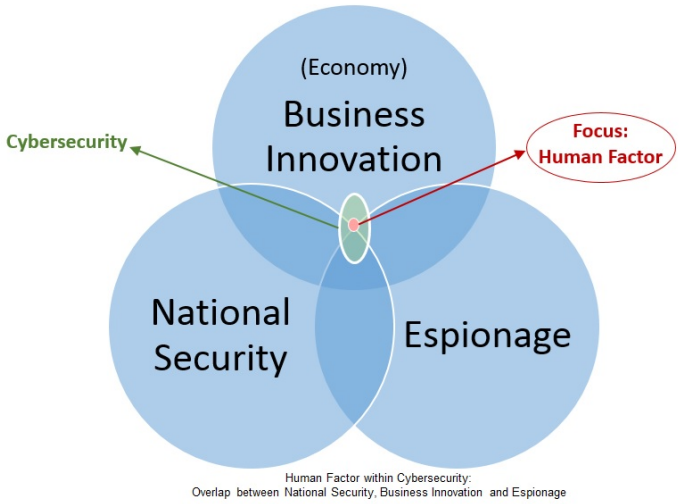
Today, in the United States, intellectual property intensive businesses support at least 40 million jobs and contribute $5 trillion to the US GDP. [6] To put this in perspective, these businesses alone have a greater GDP than Japan which has the third highest GDP in the world with a total of $4.6 trillion. [7]

National Security, Business Innovation & Espionage

Espionage encompasses a broad spectrum of interests and capabilities from various adversaries. While most would consider industrial espionage to be exclusively committed by competitors, criminals or non-state political actors, it can also be committed by nations employing state intelligence resources to commit corporate espionage in the interest of national security. This is where National Security, Business Innovation and Espionage intersect. Where national security assets include economic prosperity, national defense, geopolitical interests and socio-cultural values. Business innovation includes competitive intellectual property, business growth, reputation management, innovation capacity and capability development. When nation-states perceive it to be in their national security interests to steal foreign trade secrets, an overlap forms between business continuity, national security and espionage. It becomes a particularly sensitive discussion when businesses running critical infrastructure find themselves in the crosshairs of espionage by nation-state actors looking to degrade (sometimes disrupt) their operations, or by non-state political actors with similar intentions. Cyber criminals are active in industrial cyber-espionage having much to gain financially from the data theft. A McAfee report on cybercrime estimated that it incurred an annual cost of $445 billion to the world economy.[8] While they remain a threat, measuring the impact of hostile competitors participating in industrial espionage is challenging considering the illegal nature of engaging in theft of trade secrets. Non-state political actors can also pose a threat, in addition to data theft they can also instigate or be a part of reputation assassination campaigns against a company which can also result in revenue loss.

[4] TrendLabs APT Research Team. (2012). “Spear-Phishing Email: Most favored APT attack bait”. TrendMicro. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
[5] Get Cyber Safe. (2015). “Phishing: How many take the bait?” http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx
[6] Economics and Statistics Administration and the United States Patent and Trademark Office. (2012). “Intellectual Property and the U.S. Economy: Industries in Focus”. (http://www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf
[7] CIA. (2015). “Field Listing: GDP (Official Exchange Rate). The World Fact book. https://www.cia.gov/library/publications/the-world-factbook/fields/2195.html
[8] Center for Strategic and International Studies (CSIS). (2014). “Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II”. McAfee Report. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de



Human Factor within Cybersecurity:
Overlap between National Security, Business Innovation and Espionage

In this overlap there is space where cybersecurity and the human factor meet. It is through this lens in which this paper proposes a strategy to protect the human component of cyber security, or "the weakest link in information security" as many have called it. [9] This is an issue that is not only a concern for information security professionals and executives in the private sector, but also in the government and military. In a briefing on the state of affairs in cyber defense, Director of the NSA and Commander of the US Cyber Command, Admiral Rogers shared his thoughts on the human component of cybersecurity and said that one should "…never underestimate the impact of user behavior on a defensive strategy".[10]

There are many actors in cyberspace with malicious intent and organizations who are vulnerable for many reasons, namely because these actors are persistent, they excel at what they do and because employees are not aware of the degree in which they are targets. Organizations have responded by implementing a variety of cybersecurity strategies to protect themselves including (but not limited to):

- Network defenses such as firewalls, defense in depth approaches, intrusion detection systems and others.
- Data defenses are set up for its encryption, classification and destruction, as well as policies for data when it is in use, motion and at rest, not to mention data loss prevention plans.
- Malware defenses including anti-virus, spam filters and email filters.

But what about human defenses? Some organizations implement identity and access management policies to control access and distribution of data, and fewer incorporate operational security awareness or social engineering awareness. However, human defenses are just important as the network, data and malware defenses, as they too contribute to the business continuity and continued operations of an organization. Seeing as espionage is more often than not a human-centric enterprise, humans have a critical role to play in countering it.

[9] Schmidt, J. (2011). "Humans: The Weakest Link in Information Security". Forbes. http://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link-in-information-security/
[10] Woodrow Wilson Center. (2015). "Briefing with Admiral Michael Rogers, Commander of U.S. Cyber Command" https://www.wilsoncenter.org/event/briefing-admiral-michael-rogers-commander-us-cyber-command

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Human Defenses & Business Critical Roles (BCR)

If humans are the weakest link in information security, employees in business critical roles (BCR) are the most fragile link of them all.

For the context of this paper business critical roles are roles in an organization that are instrumental in achieving the desired goals and fulfilling aspirations set forward in the business strategy and vision. Should people in these roles be compromised it would constitute a point of failure with potentially serious to detrimental repercussions for business continuity and operations.

Business critical roles can also be viewed as: High Value Targets, Key People Terrain, (Single) Point(s) of Failure, or Nodes of Compromise. People in these roles cannot be replaced by computers or easily replaced by other people because they in themselves constitute the ideas (past, current and future) and information that cannot be easily replaced or in some cases can never be replaced. Employees in business critical roles have assets which are critical to a business' operations, continuity and innovation; as well as a business' brand. These assets can be categorized into three forms:

1. Information: Tangible and intangible information. Internal knowledge of organizational structure and operations. Trade Secrets. Business intentions.
2. Access: To data, networks, servers, people, proprietary ideas, trade secrets, money, internal strategy and intent.
3. Intellect: Innovative ideas (past, present and future), insight and perspective. Intellectual capacity and capability. Motivation and aspiration.

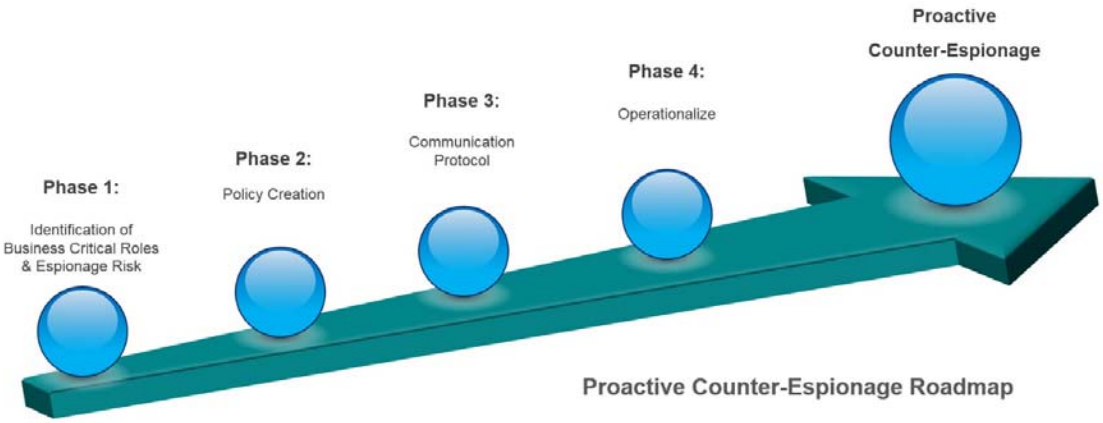
Business critical roles are the ones who are driving innovation, maintaining the organization's relevance, furthering its vision and fulfilling its objectives. The FBI's Counterintelligence Division produced a short film "The Company Man: Protecting America's Secrets" which is based on a true story highlighting the importance of people within an organization. [11] The idea that only system administrators who hold the presumed 'keys to the kingdom' are the most coveted target is a fallacy. Engineers, designers, advertisers and many others are also prime targets. As mentioned earlier in the paper, there are many actors with different intents, capabilities and agendas. It is impossible to know them all and anticipate them all, however it is possible to identify Business Critical Roles. Identifying these roles and mapping them on a network can help network managers looking at log data and assessing incidents make quicker assessments relevant to business interests. Companies that have a global reach can look at their global nodes of compromise within their organization. The following section proposes a proactive counter espionage roadmap to tie this together.

[11] FBI Counterintelligence Division. (2015). "Economic Espionage FBI Launches Nationwide Awareness Campaign". https://www.fbi.gov/news/stories/2015/july/economic-espionage

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

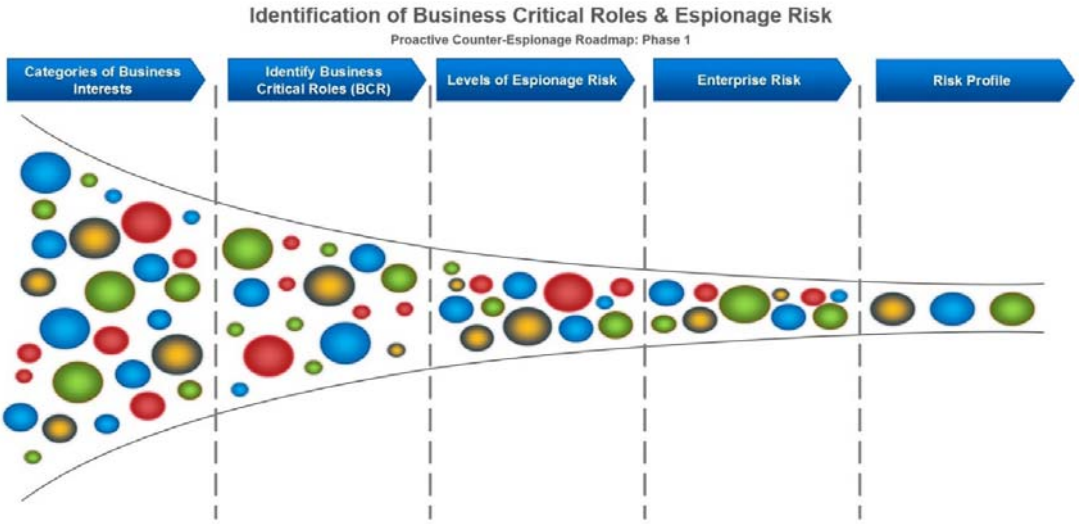
Proactive Counter-Espionage: The Roadmap

Keeping the human-centric focus of cybersecurity as it pertains to business continuity the following graphic identifies four phases to a proactive counter espionage posture which incorporates a whole of enterprise approach. The phases can be scaled to an organization's business strategy, revenue and resources. This section expands on each phase of the roadmap and identifies key tasks and actions. It should be noted that when implementing the roadmap, the analytical train of thought during this process should be kept confidential.



Phase 1: Identification of Business Critical Roles and Espionage Risk

The purpose of the first phase is to identify business critical roles vis a vis espionage risk. Business intelligence contributes to situational awareness that helps business strategies outline this phase. The following graphic shows how each element condenses strategy, roles and risk into role based risk profiles.



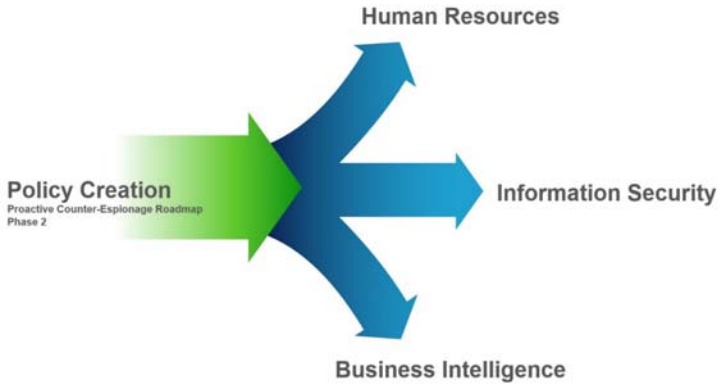
Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The following table discusses each task and its corresponding action:

Task	Action
Categorize Business Interests	Determine areas that are business critical to identified business continuity goals. This should be reflective of Business strategy, interests, goals, aspirations and continuity plan.
Identification of Business Critical Roles (BCR)	Map business critical roles on top of categories of business interests. Use business strategy as guidance.Identify people who represent business continuity points of failure in these goals should they be compromised. Identify people who represent points of failure in these goals should they be compromised.
Levels of Espionage Risk	Define levels of espionage risk from low (1) to high (5). Collaboration with Business Strategists, Business Intelligence and Security Operations. Risk levels should be defined as per impact to business interests, incorporate business intelligence and reflect organization's risk appetite.
Enterprise Risk	Define BCR roles within categories and risk levels specifically as they pertain to the respective business. Definitions should clearly indicate the criticality of role responsibilities and the value the people in these roles bring to achieving desired business goals, as well as the risk for business continuity should they be compromised. Business strategy, risk appetite, people & threat analysis should be incorporated.
Risk Profile	Prepare tailored risk profiles of business critical roles to be delivered for situational awareness, policy creation and need based use by: Business Strategists Human Resources Business Intelligence Security Operations Information Security

Phase 2: Policy Creation

The second phase determines policy creation for relevant departments within the organization namely HR, IT and business intelligence. Cybersecurity is truly a team sport and policy creation, to protect employees in business critical roles from adversaries intending to steal corporate secrets, should not be left solely in the hands of the information security department. Human resources and business intelligence can work hand in hand to further a human-centric counter espionage strategy.



Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Human Resources. Using the role based risk profiles created in phase one, human resources along with business strategists develop an internal classification typology of high espionage risk roles and responsibilities. Hiring policies for roles identified as high espionage risk should be created with cross-departmental collaboration incorporating business intelligence.

Information Security. Along with business strategists and business intelligence analysts, the information security department leverages the role based risk profiles tailored for their department to create espionage risk based policies for:

- Identity and access management.
- SIEM policies for life-cycle of employee and role type.
- Establish defined 'need to know' events relating to employee.
- High espionage risk employees' device policy.

Business Intelligence. Business intelligence analysts develop policies for additional intelligence gathering and production relating to espionage risk roles and coordinates with Human Resources when needed during the hiring process of such roles. Policies are created for:

- Operational Security (OPSEC) Audits.
- Establish BCR related policies to preserve, protect and maintain operational security (OPSEC).
- Big data/intel feedback loop protecting BCR employees.
- Reverse Open Source Intelligence (OSI) Hunting.[12]
- Sanitation of compromising open source information as well as Publicly Available Electronic Information (PAEI).

As policies are created in this phase, the security culture of an organization should be assessed for its level of awareness and proactivity to counter threats.

A heightened user's sensitivity to espionage contributes to maintaining readiness. When incorporated into organizational security policy awareness programs can contribute to the hardening of human assets[13] similar to when technical measures are implemented to harden a network or computer. The following awareness programs are beneficial to employees in roles deemed to be of high espionage risk:

- Data protection awareness
- OPSEC Awareness
- Social Media Use Awareness
- Social Engineering Awareness
- Espionage Threat Awareness
- Travel Security Awareness

[12] Reverse Open Source Intelligence Hunting – Similar to cyber hunting which is implemented to proactively search and identify unusual activity in the cyber environment to gain a better picture of the technical cyber environment; reverse open source intelligence hunting searches the open source domain for unusual activity, unauthorized information dissemination, hostile social network discussions, and unintended leaks, etc, that adversely affect organizational interests in efforts to gain a better picture of the human cyber environment.
[13] Hardening of Human Assets (HHA) – The process of elevating security awareness of a human asset in efforts to reduce and eliminate as many risks as possible.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Phase 3: Communication Protocol

The third phase assesses best practices for communication protocols when implementing the policies identified in phase two. Additional communication protocols should exist to address latest trends in cyber-attacks.

One of the cyber-attack trends that has gained momentum is the 'CEO Fraud' where the attacker impersonates the CEO of a company in a spoofed email requesting that the recipient transfer a certain amount of funds to a designated bank account. Companies have lost millions of dollars to this scam.[14] For example, one way to help mitigate this type of risk is to create a communication protocol for all employees with authorization to initiate bank transfers on behalf of the organization outlining the organizational stance on wire transfer requests by email. Another communication protocol that could be set in place to counter this threat is create a method of cooperation to share the CEO's calendar with the information security department so they can act in accordance with relevant organizational policies and attack trends. Cross departmental communication is becoming more important than ever before as adversaries attempt to penetrate through the weakest link (the human).

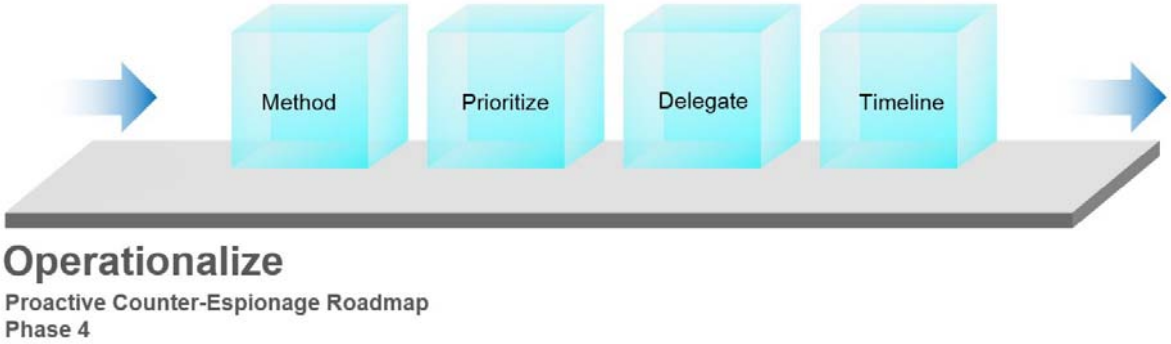
As Heraclitus the ancient philosopher said "The only thing constant in life is change". Adversaries will continue to deploy innovative attacks utilizing new attack vectors. The best way to mitigate this is to be agile and adapt to constantly changing circumstances while keep the channels of communication open.

Phase 4: Operationalize

Phase four offers guidance on steps to operationalizing the roadmap. The first step would be to determine the best method for implementing the roadmap. This would include identifying a chain of command for operationalizing the roadmap with key stakeholders. Part of the method step should be to assess what steps should be taken based on the unique culture, operations and resources of the organization in question. Lastly it should detail a list of tasks to be done.

[14] Hackett, R. (2015). "Fraudsters duped this company into handing over $40 million". http://fortune.com/2015/08/10/ubiquiti-networks-email-scam-40-million/

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de



The following step would be to prioritize the identified tasks into essential tasks, primary and secondary tasks. These categories would need to be decided by those at the top of the chain of command for operationalizing the roadmap. Once the tasks have been prioritized then they need to be assigned to people who will be responsible for their completion and oversight. All those involved in this phase will need to agree on a suitable timeline for operationalizing the roadmap which will vary based on the time constraints and resources of the organization.

Once the roadmap has been tailored to an organization's needs and the proactive measures have been set in place, a system for monitoring the measures implemented as well as reporting them should be determined. A KPI (Knowledge Performance, Indicator) could also be included if needed/desired.

Concluding Comments

This white paper has presented a proactive human-centric counter-espionage approach which contributes to an organization's overall security posture and helps protect business interests and continuity. The outlined road-map is a moldable and scalable process which can be tailored to an organization's respective strategy, interests, resources and threats. It is important to keep in mind that just as our adversaries are relentless in acquiring our data, we should be relentless in protecting it.

***

Remarks: Opinions expressed in this contribution are those of the author.

This paper was presented at the RSA Conference in Abu Dhabi on November 5th, 2015 at Emirates Palace.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

About the Author of this Issue

Dr. Lydia Kostopoulos teaches intelligence and cyber security at the Institute of International and Civil Security at Khalifa University in Abu Dhabi. In the US she is the International Engagement Coordinator for the Cyber Security Forum Initiative participating in global cyber efforts. Prior to her move to the UAE she was a professor teaching at the American Military University's Intelligence Studies Department.

She regularly engages in the American cyber community as part of CSFI, in law enforcement as a member of FBI's InfraGard and in the military participating in training and exercises in multi-nation environments. Internationally she has participated in NATO's Science for Peace program where she recently conducted a workshop on social engineering awareness and its implications for national security. She has been awarded the Presidential Service Award for collaborative efforts and service to the cyber community.

Lydia Kostopoulos

@LKCYBER

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de