Unintentional Insider threat: Policy, training and technologies to mitigate end user risk

Alejandro Mera

IA5010 Foundations of information Assurance

April 19, 2015

Introduction

Information Security researchers have evidenced that end users remain the greatest Security Risk for information in the last five years (Karr 2015) (Ponemon Institute 2012). Moreover, their findings suggest that not only malicious activities are related to end user risk; for instance, one of the biggest concerns is the unintentional insider, whose non-malicious actions could harm or expose organization's assets. Similarly, The State of the Endpoint Report: User-Centric Risk, a report produced by Ponemon Institute, states that 78% of respondents consider negligent or careless users who do not follow security policies as the biggest threat to endpoint security (2015).

The unintentional insider threat (UIT) is not an isolated fact; consequently, many other threats have been linked to the increase of end point incidents, and an operational definition of UIT has been developed (CERT 2013); however, it is essential to understand the relation of UIT to other contributing factors and the correcting actions taken by organizations to control this threat. This knowledge would help IT practitioners to develop effective UIT mitigation strategies that conform a comprehensive security plan.

The human factor and contributing factors of UIT involve management and technical issues; therefore, a set of policy, training and technologies, must be included in an effective security plan to mitigate UIT rather than an isolated solution. Moreover, this approach considers people as the beginning and the end of information and includes the three principal categories of controls used to protect the critical characteristics of information (confidentiality, integrity and availability) (Michael E. Whitman 2012).

Unintentional insider overview

A UIT is an individual who has or had legitimate access to an organization's information, and who, through action or inaction without malicious intent, unwittingly causes harm or exposes the CIA characteristics of the organization's information (CERT 2014). This definition, developed after the research of Computer Emergency Response Team (CERT), states a direct relation with a human factor or end user, and suggests the absence of two features: maliciousness and intention. These are key aspect that differentiate the UIT from the malicious insider threat.

Threats and contributing factors

Whitman considers that "people always have been a threat to information security" (2012), and this issue could be represented with many accidental or intentional actions or inactions that affect the CIA characteristics of the information. However, in the context of this report, only human error, negligence and aggravating technologies are contributing factors to UIT.

Negligence, Human error

The direct relation between UIT and people suggests that human activities and behavior are the principal contributing factors for this threat. Recent research states that clicking on suspicious URLs and opening suspicious attachments are the end-user behaviors that represent the source of the most security risk (Karr 2015). Figure 1 depicts the result of a survey, when security information professionals responded about what end-user behaviors are the source of the most risk.

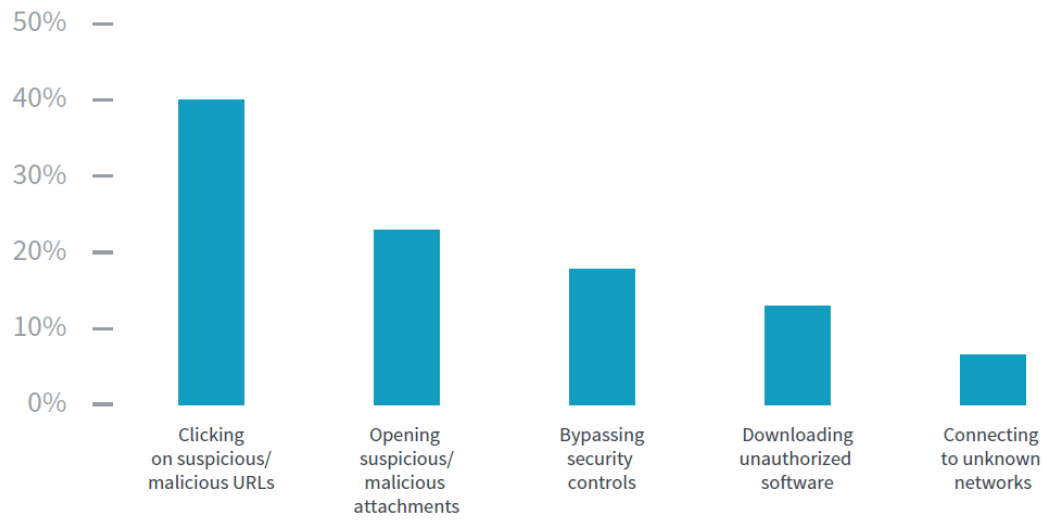

Figure 1. End user behavior as source of end user risk, Data from Karr 2015.

As shown in Figure 1, the third category 'bypassing security controls' is not considered a threat related to UIT, because this behavior implies intentionality and it has been more likely related to the intentional insider. Actually, CERT defined four categories for UIT incidents: accidental disclosure of information, phishing /social (2014), improper or accidental disposal of physical records and portable equipment no longer in possession (CERT 2013).

Many of the human contributing behaviors identified on Figure 1 share common characteristics with human error, ignorance, and policy breach. For example, an untrained employee is likely to click on a suspicious URL, because he does not have the knowledge to recognize the threat or because he is unaware of security policy related to restrictions of access to unsecure sites. However, a trained employee, under pressure or other factors, could click on the suspicious URL accidentally, regardless of the training he received. A recent survey reveals that untrained or careless employees are the biggest threat to endpoint security (Ponemon Institute 2015), while an extensive research of CERT suggests that "behaviors such as anger, disgruntlement, stress, etc. may provide indications of more deep-seated

psychological/psychosocial issues that could negatively impact the employee's perception of risk, risk tolerance, and decision making performance" (2013).

Phishing/Social

Phishing/Social is a parent-threat that includes the sub-threats of malware and compromised credentials. Initial studies of security incidents stated that malware was a principal vector category related to UIT (CERT 2013), but further research and new information collected suggest that phishing/social threat is a parent vector attack that is virtually common to all incidents related to malware and compromised credentials. Therefore, Phishing/Social was established as one of the four principal categories of UIT incidents (CERT 2014).

In the context of UIT, phishing/social differs from other categories described by CERT, because it is the only one that requires an outsider—attacker—as a precursor, who uses social engineering to reach the unintentional insider; in other words, the outsider takes advantage of an internal human error. The willingness of users to click on malicious URLs is the most common human behavior that an outsider uses to exploit the Phishing/Social threat, and emails or untrusted websites are the method to deploy malicious URLs as part of a social engineering attack. In fact, a recent survey pointed out that Web-borne malware and spear fishing are among the more common attacks experienced by IT organizations in the last four years (Ponemon Institute 2015).

Mobile devices

Improper or accidental disposal of portable equipment no longer in possession is the threat that involves mobile devices. Portable equipment traditionally includes laptops, USB flash drives, external HDD and a special category related to smartphones and tablets (CERT 2013). This last category elicits a special interest, because self-owned mobile devices (smartphones and

tablets) are increasingly used within organizations with no favorable consequences associated with the organization's security. Many studies suggest that organizations will have a substantial increase in the use of mobile devices in the following years (Ponemon Institute 2012); aditionally, security practitioners believe that use of mobile devices has increased end-point risk (Ponemon Institute 2012), and this tendency will continue in the following years. (Ponemon Institute 2015).

Cloud Services

This thread includes all the third party applications or services (file sharing, social media, development, collaboration, business intelligent, tracking and content sharing) that unintentional insiders use within an organization where cloud solutions are popular among employees. The reasons for popularity of cloud services include collaborative environments with multiple synchronized devices—functionalities not offered by legacy software, and relatively low fees. In this case, Skyhigh Networks showed that an average employee uses twenty-seven different cloud services including three different services for file sharing (2014). Moreover, the principal incident related with the use of cloud services is the accidental disclosure of personal or corporative information; in fact, cloud file sharing and social networks are largely recognized as a threat to personal and corporate information when these services are used without responsiveness. For instance, a study with user's data from cloud services (not a survey-based study) revealed that 22% of files uploaded to a file-sharing system contain sensitive data (Skyhigh Networks 2014).

Strategies to mitigate UIT

Human behavior and lack of intentionality are key factors that characterize UIT; therefore, the strategies to mitigate this threat have to consider the absence of personal motivation—financial need, anger/revenge, ideology, trill and divided loyalty are personal motivations related to intentional insider that are not applicable for UIT (FBI 2012). In addition, the "psychological/psychosocial issues" are key concerns that an effective strategy has to address in order to reduce human error as a contributing factor of UIT.

Case of study: Global Manufacturing Company Reduces Malware infection

Information about company's security events is normally secret, because its disclosure can affect company's image. However, the information of cases that are publically available or retrieved by research institution like CERT constitutes a rich material to understand UIT, for instance causes of security events, threats and mitigation strategies are the most important parts of a security event case.

Case Abstract:

A large international equipment manufacturer based in Pennsylvania has a very strict email authentication program in place for incoming messages; however, it is not effective at preventing phishing emails. Employees were falling for scam messages, clicking suspect Internet URLs, and visiting malicious websites. Naturally, these activities had a negative impact on the company's internal systems. They reported 70 malware infections a day worldwide that represent a remediation cost at $700,000 per year. The company decided to implement a global tailored security training program using both interactive educational modules and threat assessment. The awareness program included: safer web browsing, email security, URL training, and simulated attacks. The result showed an overall 46% reduction of malware infection, while the European

branch saw the most significant reduction with a 69% after 4 months; it represents $300,000 in annual savings. (Wombat Security Technologies 2014)

Analysis:

This case is an example of the UIT phishing /social category, where the principal vector attack is phishing emails that contain malicious URLs in order to deploy malware or to perform other social engineering attack (theft of credentials and scams). The identified causes for this incident are three: inefficiency of the authentication technology at detecting phishing emails, unawareness of the employees and a probable lack of security policy.

The strategy used to mitigate the threat include security awareness program (education and training) and threat assessment. This approach tries to cover the company's technological weakness, and relies its effectiveness on security programs; however, there is no clear evidence of development or enforcement of information security policy.

Information security policies

The information security policy is the basis of all information security initiatives, because it states how information assets should be protected and how technologies should be used for the sake of the organization's interests. The security policy is a very important control to mitigate the UIT; many studies suggest the development of specialized security policies, as a method to address the endpoint risk related to the increasingly use of mobile devices (BYOD) and cloud applications (Ponemon Institute 2015) (CERT 2013). Similarly, accidental data breaches could be mitigated with adequate policies. For example, Boston Children's Hospital, after being involved with a data breach for a stolen hospital-issued unencrypted laptop, worked with government authorities as well as security experts to ensure that its security policies are effective to prevent a data breach from happening again (Modern Healthcare 2014).

The effectiveness of policy as a control depends on its intrinsic definition; in other words, the policy's statements have to address the specific contributing factors of UIT (mobile devices, cloud applications and human factor). Besides that, research performed to highlight policy's strengths and weaknesses when considering the prevention of UIT, suggests that the best studied policy covers only 80% of the reasons (data exposure, misconfiguration of resources and security training) and 86.7% of the actions associated with UIT (e.g. disposal of resources, use of mail and data protection) (Oliver Buckley 2014). For example, a policy to avoid human errors (actions associated with UIT) must include optimal working conditions (temperature, light and noise level) and schedule with specific working and odd periods. This policy ensure that employees perform their activities in a favorable environment and maintain adequate risky perception during working hours—human contributing factors of UIT. Moreover, overtime work, weekend work or unusual schedules are behavioral indicators of malicious insider (FBI 2012); which intentions differs from UIT, but their environmental conditions can be common.

A drawback of policy as a control is that technical and management processes are necessary to assure policy enforcement, that means security policies needs the involvement of IT, legal, financial, human resources and executive levels of a company, whose decisions must include information security as a part of company's strategy. Consequently, Whitman considers policy as the "least expensive control to execute, but the most difficult to implement *properly*" (2012); this claim reminds of the difficulty of implementing a policy that is consistent with law, formally accepted, widely distributed, and applied. Furthermore, literature related to risk suggests the difficulty of enforcing endpoint policy as a contributing factor to endpoint risk (Ponemon Institute 2015). As shown in Figure 2, the gaps that security practitioners believe they are facing at stopping end-point attacks are the lack of governance and control process.

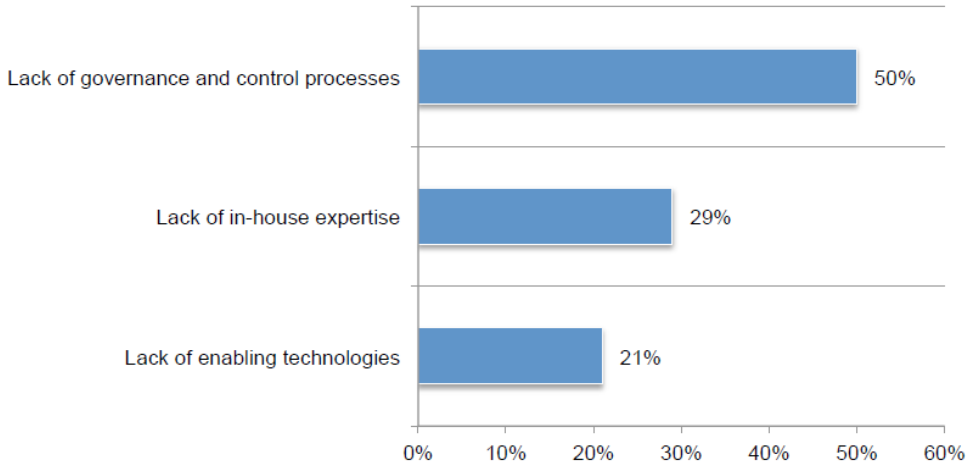

Figure 2 Gaps in the ability to stop attacks to endpoints, Data from Ponemon Institute 2015.

Training, education and awareness programs

The principal objective of education and training is to give individuals knowledge and skills that enable a behavior and culture of security awareness while performing daily activities. In other words, training and education are methods to protect information delineating processes and activities that improve the decision-making and risk-perception of individuals. For instance, UIT could involve repetitive daily activities that are considered safe, when in actuality, those actions are the motive of two events: putting information security at risk and increasing advanced persistent threats (APT).

The Chinese hacking attack to the New York Times in 2012, which was a broadly publicized event, is a case of UIT that triggered an APT. After more than four months of investigation, security specialists determined that many computers were infected many times with malware delivered by phishing emails. Consequently, security remediation efforts to change and clean infected computers were ineffective, because UIT (phishing/social) was not mitigated. Asked about the time it took to detect the attack and implement the corrective actions; Marc Frons (Chief Information Officer at The New York Times) said, “Some of the antivirus programs

don't really work anymore… there are many things we can do with technology—hardening of systems to make them more secure. But a lot of the ways that hackers get in is with a phishing email... so what we really want to do is to raise the awareness of everyone on the company" (New York Times, the 2013). Frons believes that technological solutions are not the only solutions necessary to mitigate UIT; rather he claims antivirus software is not effective anymore and highlights awareness programs as the solution to protect information. That opinion is shared among many security professionals which believe antivirus software is still important, but nowadays it is just one of many technologies to keep computers safe (PC World 2014).

An awareness security program can address the technological weaknesses with elements that include recognizing phishing emails and malicious URLs, enforcement of policy, training to use software and hardware within an organization, awareness of risk, and management of printed or digital information (CERT 2014).

Enabling Technologies

In the context of UIT, enabling technologies are devices that provide automated defense as a complement to policies and training/education programs. CERT defines these technologies as automated fail-safe safeguards against the failures of training and cognitive recognizance of risk (2013); therefore, these technologies must offer "detect and respond" capabilities rather than preventive ones. Naturally, these technologies must concentrate on end users and their tools. In fact, a popular trend among security solution vendors is to use "endpoint as a security sensor", which means information gathered at endpoint is used to determine an unusual activity (Ponemon Institute 2015).

Some of the commercially available technologies to mitigate UIT include enhanced endpoint solutions, malware detection system, antivirus software, email filters/firewall, intrusion

prevention systems (IPS) and a new generation of technologies that use data analytics to tackle the UIT. For example, Security Information and Event Management (SIEM) and Data Loss Prevention (DLP) use big-data analytics to discover, monitor, protect and manage sensitive information wherever it is stored and used (endpoints, network and storage systems). In fact, a recent Ponemon Institute's survey reveals that 33% of respondents say they have added a threat intelligence component to its security infrastructure and 59% of respondents say they are planning to use big-data to enhance their security systems in the following two years (2015).

The use of modern technologies can help security personnel to identify human activities that fall outside the boundaries of security policy and common sense. However, these technologies must restrict improper behaviors rather than just trigger alarms. A recent research suggests that technology can educate and disseminate good practices through restrictions and alarms that clearly block activities and show alerts of risky behavior to users; especially, when these activities do not involve malicious intention (IS Decisions 2015). Accordingly, an article that describes Target's data breach in 2013 revealed that this attack was preventable after Target's malware detection system alarmed the security team, but the security specialists did not react and neither the automatic malware defense was enabled (quarantine and malware removal). Asked about the incident Target CEO Gregg Steinhafel said, "Target was certified as meeting the standard for the payment card industry (PCI) in September 2013. Nonetheless, we suffered a data breach. As a result, we are conducting an end-to-end review of our people, processes and technology to understand our opportunities to improve data security…" (Bloomberg Business 2014). This shows that a technological security solution (malware detection system) needs trained people—including technical personnel—and adequate incident respond plan (policy, processes and procedures) to be effective against UIT.

User centric management risk

The security UIT events involve human actions and tools—software and hardware—that people use to perform their activities; this relation between tools and UIT agents generates a specific risk localized at endpoints (workstations, personal computers, laptops, smart phones, tablets, bar code readers, printers, scanners, point of sale (POS) terminals, kiosks, IP phones and Wi-Fi access points). In other words, UIT thrive in places where the end user generates, interchanges and consumes information. For example, a phishing email—UIT phishing/social category—acts in personal computers or mobile devices where the end user reads his e-mails. In fact, Ponemon Institute's "Post breach boom report" reveals that 63% of non-malicious (unintentional) data breach compromises endpoints (2013). As shown in Figure 3, the most common assets compromised by unintentional data breach include endpoints, databases/users accounts.

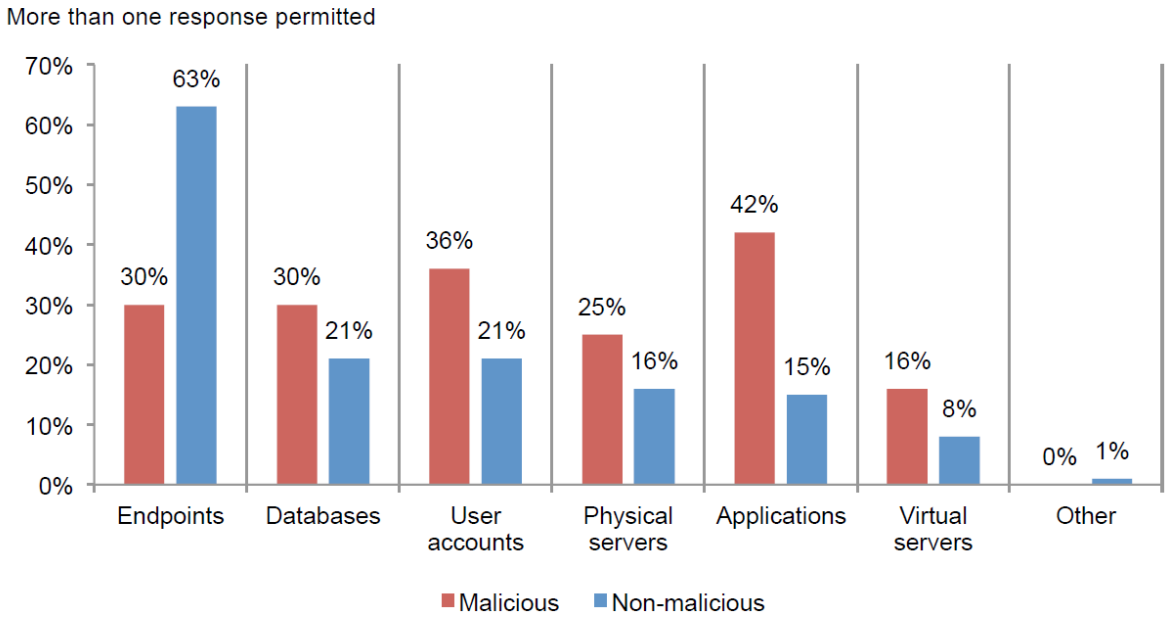

Figure 3 Compromised assets by data breach, Data from Ponemon Institute 2013.

Conclusions and future work

Researchers and security practitioners have recognized that unintentional insider, who lacks motivation and intentionality to cause damage, is one of the biggest threats to information security. Moreover, the direct relation of UTI to human error—a intrinsic characteristic of human activity—and contributing factor such as lack of policies, cloud applications, mobile devices, and unawareness have jeopardized the risk related to this threat. For instance, this paper showed many documented cases and studies that revealed untrained or negligent employees, stolen mobile devices, file sharing services (cloud services) and failing processes as the cause of many security events or repetitive infections in events that involve advanced persistent threats (APT).

The analysis of cases of study, and evidence retrieved from research reports suggest that many organizations, after suffering data breach or attacks related to UIT, have implemented combined strategies to mitigate UIT risk. Moreover, none of the analyzed cases has suggested a unique approach to tackle UIT. For example, organizations that suffered repetitive phishing attacks have updated its technology stack and implemented security awareness programs, whereas organizations that were involved with data breach have revised its processes and trained its employees.

The presented evidence suggest the following set of solutions to tackle UIT:

- Specific policies that concentrate on the contributing factors of UIT (human factor, mobile devices and cloud applications) and control processes to enforce the policy.
- Training that helps to cover the weaknesses of technological solutions (security awareness program and threat assessment).

- Enabling technologies that act in a “detect-and-respond” way using the endpoint as a source of sensing information and big-data (SIEM and DLP technologies) to detect unsafe activities of employees.

The present paper is limited to public available information of cases of study, research reports and recognized literature; furthermore, the private character of information security events and the consequences of the disclosure of this demand a great compromise of institutions that collect and have access to this information like CERT, which is a recognized authority in the study of UIT. Future research should focus on empirical evaluation of the proposed strategies because there is no public information that reveals measurable effectiveness of them.

Bibliography

Bloomberg Business. *Bloomberg BusinessWeek.* March 13, 2014. http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1 (accessed April 8, 2015).

CERT. *Unintentional Insider Threats: A Foundational Study.* Insider Threath Team, Carnegie Mellon University, Pittsburgh: Software Engineering Institute, 2013.

———. *Unintentional Insider Threats: A Review of Phishing and Malware Incidents by Economic Sector.* Carnegie Mellon University, Software enGineering Institute, 2014.

FBI. *The Insider Threat An introduction to detecting and deterring an insider spy.* 2012. http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat (accessed March 22, 2015).

IS Decisions. *The Insider Threat Security Manifesto.* Research Report, Bidart: IS Decisions, 2014.

———. *User security in 2015: The future of addressing insider threat.* Research report, Bidart: IS Decisions, 2015.

Karr, Clinton. *Endpoint Protection Attitudes & Trends 2015.* Cupertino: Bromiun, 2015.

Michael E. Whitman, Herbert J. Mattord. *Principles of Information Security.* Boston: Course Technology, Cengage Learning, 2012.

Moberly, Michael D. *Safeguarding Intangible Assets.* Waltham: Butterworth-Heinemann, 2014.

Modern Healthcare. *Boston Children's Hospital settles over data breach.* December 22, 2014. http://www.modernhealthcare.com/article/20141222/INFO/312229932 (accessed March 22, 2015).

New York Times, the. *The New York Times.* 01 30, 2013. http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=1 (accessed 03 15, 2015).

Oliver Buckley, Jason R. C. Nurse, Philip A. Legg, Michael Goldsmith, Sadie Creese. *Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat.* Department of Computer Science, University of Oxford, Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on, 2014.

PC World. *Antivirus is dead, says maker of Norton Antivirus.* May 05, 2014. http://www.pcworld.com/article/2150743/antivirus-is-dead-says-maker-of-norton-antivirus.html (accessed March 12, 2015).

Ponemon Institute. *State of the Endpoint.* Research Report, Ponemon Institute, 2012.

———. *State of the Endpoint Report: User centric Risk.* Ponenom Institute, 2015.

———. *The Post Breach Boom.* Research report, Ponemon Institute, 2013.

Skyhigh Networks. *CLOUD ADOPTION & RISK REPORT.* Skyhigh Networks, 2014.

Wombat Security Technologies. *Global Manufacturing Company Reduces Malware Infections by 46%.* Pitssburg: Wombat Security Technologies, 2014.

Foundations of Information Assurance Paper Outline

I would like to research risk controls to mitigate the information security risk due to end users. I want to study which vulnerabilities and attacks are related to end users and what strategies are being applied to mitigate risk. My goal is to understand why combined risk controls (policy, programs and technologies) are necessary to address end user information security risk.

I. Introduction: Combined risk controls are necessary in order to mitigate end user information security risk
   a. Information Security and risk management
   b. Risk Control
II. Vulnerabilities and information security threats related to end users
   a. Negligence, ignorance
   b. Use of private cloud applications
   c. Mobile devices
   d. BYOD
   e. Malware
      i. Increase of endpoint malware
III. Three different risk control categories to mitigate end user risk
   a. Enforcement of endpoint security policies
      i. Governance
   b. Training and awareness programs
      i. Education
   c. Enabling technologies
      i. Endpoint security software
      ii. VPN

IV. User centric management risk approach
   a. End users the greatest threats to information security
   b. The shift from endpoint risk to user centric risk

V. Conclusion: The presented evidence is substantial to indicate the necessity of policies, programs and technologies to mitigate end user information security risk.