Human and organisational factors in cybersecurity: applying STAMP to explore vulnerabilities

Andrew Wright[1], Gyuchan Thomas Jun[2]

[1]Corporate Risk Associates, [2]Loughborough University,

ABSTRACT

The human and organisational factors contributing to information security are still poorly understood, primarily due to a lack of research and absence of suitable techniques to assess complex digital systems. This paper presents the application of the System-Theoretic Accident Models and Process (STAMP) technique to the 2013/2014 Target Corporation data breach. The aims of the study are to investigate the causal factors using a systemic approach, and to demonstrate the benefits of the technique to information security applications. A number of critical control flaws were identified through the STAMP analysis include: i) poor external and internal communication/co-ordination of new threats and vulnerabilities; ii) inadequate learning from past events, internally and externally; iii) a lack of proactive security management to understand and learn from system successes and good practices as well as system failures; iv) ineffective management and co-ordination with the supply chain.

KEYWORDS

Information Security, Cyber Security, STAMP

Introduction

The importance of information security and the requirement to design resilient security systems is arguably one of the greatest technical challenges of this century. In a highly connected world, organisations and their workforces require flexibility and adaptability to prevent or mitigate security threats that are engineered to exploit human vulnerabilities and can result in catastrophic damage, ranging from financial and reputational losses to public safety and potentially, loss of human life. Mitigation against threats is best achieved using holistic assessments of sociotechnical systems and the human and organisational factors that, if mismanaged, result in costly incidents (Kraemer et. al., 2009).

Information security traditionally focuses on technological solutions for risk mitigation (Besnard and Arief, 2004), however there is an increasing recognition of solutions that assess information security as sociotechnical systems (Kraemer and Carayon, 2003; Liginal et. al, 2009; Hauer, 2015) to explore the human and organisational factors behind incidents (Dhillon and Backhouse, 2001). Whilst these factors are understood in the operation of safety-critical sociotechnical systems (Rasmussen, 1994; Reason 1997), the literature review suggests that they are not yet thoroughly understood in information security (Kraemer and Carayon, 2003), which is primarily due to a lack of effective techniques (Hagen et. al., 2008; Lee, 2012). A number of tools are being developed or

adapted to the security domain to address these need, including the System-Theoretic Process Analysis (STPA) tool which has been dubbed STPA-Sec (Young, 2014; Young and Leveson, 2014).

It is considered that other systems-theory techniques would be equally suitable to address the lack of security risk management tools (Kraemer and Carayon, 2003; 2009). This paper explore the suitability of the 'System-Theoretic Accident Models and Process' (STAMP) technique. STAMP is a systems-theory causal analysis model that analyses where external disturbances or dysfunctional interactions among system components are not adequately handled by the control system (Leveson, 2004). STAMP views accidents as failures to adequately control system constraints on the design, development, operation and maintenance of the system. Using this philosophy, STAMP assesses how control loops degrade and migrate the safety/security margin from equilibrium towards a vulnerable state of elevated risk. Unlike traditional safety-based models, STAMP was designed to assess modern complex systems that possess high coupling, integrated computer technology and human-automation relationships (Leveson, 2002). These characteristics feature strongly in information security systems, which are highly digitalised and often rely upon a combination of automated systems and human operators to gather threat intelligence and respond to attacks, and therefore often consist of multiple human or automated controllers acting on tightly coupled processes.

This study explores how STAMP can be applied to an information security breach case study to identify the control system interactions and flaws that led to the incident. This study will consider the effectiveness of applying these safety-domain techniques to address current gaps in information security risk assessment techniques by comparing the findings against other incident reports and assessments of the breach.

Target Data Breach

Target did not release complete details of the 2013/2014 breach, Therefore analysis has been collated and cross-checked using publically available information, from Jarvis and Milletary (2014), Radichel (2014), the US Senate Committee on Commerce, Science and Transportation Report (2014), and Shu et.al. (2017). Publically available news reports (e.g. KrebsonSecurity, DarkReading) were also used.

The Target security breach was the largest of its time and resulted in over 40 million customer credentials stolen from Point of Sale (POS) systems across 2000+ stores (Radichel, 2014), resulting in substantial financial and reputational losses. Figure 1 presents a timescale of the event (Jarvis & Milletary, 2014).

Attack trends for similar breaches at US retail organisations in 2014 (Hawkins, 2015) demonstrate that extensive reconnaissance would have been performed prior to the attack. Publically available data on the Target security infrastructure and the supply chain would have been analysed. An advanced persistent threat (APT) campaign would have subsequently been conducted on Target's supply chain (Chen et. al., 2014), utilising personalised 'spear phishing' techniques (Hong, 2012) to coerce security information from individuals. Supply chain organisations typically do not have the level of cybersecurity resources when compared to larger organisations, but can possess direct access to large corporate networks. On this occasion a refrigeration vendor, Fazio, was compromised and malicious software installed on Fazio machines to obtain passwords and information for Target's vendor portal, Ariba.

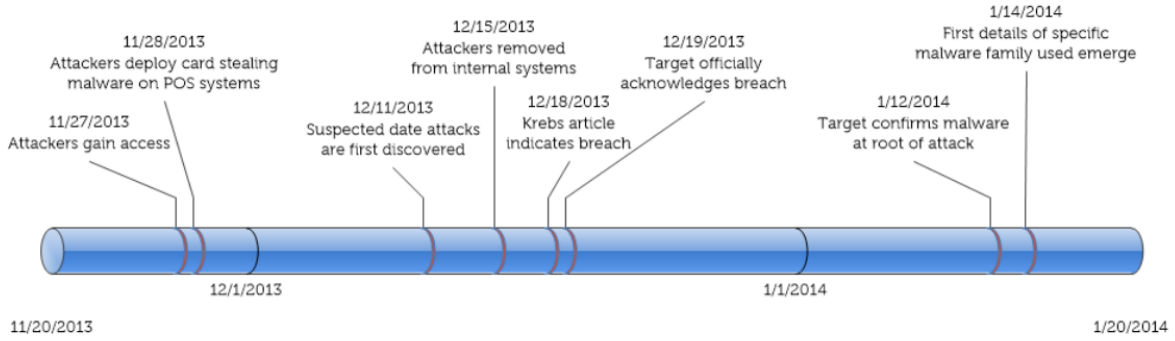

Figure 1 – Target Data Breach Timeline (Jarvis & Milletary, 2014)

Ariba was part of Target's overall IT infrastructure, but was designed to be isolated from Target's central 'corporate network'. Despite this intention, attackers were able to pivot from Ariba onto the corporate network by uncovering preventable domain controller vulnerabilities and misconfigurations. Attackers were subsequently able to probe the corporate network and obtain administrator credentials and privileges. These activities identified areas of the network which were poorly configured, i.e. default user names and passwords, or where two-factor authentication (2FA) was missing.

The attacker's thorough understanding of the network was demonstrated by the creation of bespoke software to hijack Target's patching service with a RAM scraping kit (Hizver and Chiueh. 2011). After concealing this malware within the service, it was covertly distributed to POS systems across Target stores and gathered credit card information from memory as cards were swiped for payments. Stolen information was gradually pooled into a single compromised machine on the corporate network and then extracted.

Whilst the attack was sophisticated and utilised zero day vulnerabilities (Bilge and Dumitras, 2012), Target's third-party Security Information and Event Management System (SIEMS) had detected suspicious activity within the network, and alerted Target staff to the threat. The attack was allowed to continue and ultimately succeed due to a failure by Target to respond to these alerts over several months, representing one of the most significant security failings, which was the subject of extensive media coverage.

STAMP Analysis

STAMP introduces the concept of 'control flaws', which constitute the ways in which control loops can erode, interact or fail to operate as intended such that the security constraints placed on a system are compromised. Hazards are defined as a "system state or set of conditions that, together with a particular set of worse-case environmental conditions, will lead to an accident" (Leveson, 2011).

Safety requirements and constraints

To understand how control flaws occurred in Target's information security systems, it is necessary to analyse the safety requirements and constraints of each actor. Whilst it cannot be conclusively determined which specific constraints each actor aimed to impose and to what extent they satisfied themselves that this had been achieved, a high level summary of constraints on four actors can be surmised and is presented in in Table 1.

Table 1: Security Constraints and Requirements for key Target Stakeholders

Actors	Safety requirements and constraints
Retail Industry Regulator	1) Define industry cybersecurity requirements and best practices. 2) Ensure that the collective industry maintains resilient against cybersecurity threats. 3) Oversee/enforce security auditing 4) Outline criteria for organisations at risk.
TARGET Management	1) Interpret and oversee compliance with regulatory and legal cybersecurity requirements, including auditing. 2) Ensure organisational and customer data security is adequate. 3) Provide adequate policies, processes, management systems and resource for cybersecurity. 4) Report security breaches to regulatory bodies, security authorities and general public. 5) Oversee organisational training and awareness raising campaigns.
TARGET Security Operator	1) Ensure organisation and customer data are adequately secured using organisational resources, policies and processes. 2) Configuration of network security systems. 3) Change management and vulnerability management of network. 4) Actively detect, monitor, escalate and respond to security threats. 5) Enforce information access control on network. 6) Monitor SIEMS output and network activity. 7) Ensure that unauthorised users can not access the network.
Supply Chain Organisations	*(Identical to Target Management and Target Security Operations Team)*

Target corporate management had overall responsibility for customer data relating to transactions at Target and were therefore responsible for organisational policies, processes, acquisitions and recruitment to ensure that information security systems adhered to federal law. Target possessed an internal auditing team (Schwartz, 2013) including Payment Card Industry (PCI) compliance for POS systems.

Target internal security operations team implemented information security measures within the organisation (Radichel, 2014). Responsibilities would have included establishing risk management systems, user account control, passive security software, training, patching regimes and network configuration. Target outsourced SIEMS management to a third party security organisation and did not utilise a manned SOC to monitor network activity, but would have performed active monitoring within their team.

Target's supply chain organisations were responsible for their own compliance with information security regulations and law. It is not thought that Target placed additional security requirements on their supply chain to ensure homogeneity.

Regulatory responsibility for information security in the United States is split between various organisational bodies relating to specific industries. The main regulatory bodies involved in overseeing information security for Target are the US Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC). Together, these organisations act to provide industry

regulation, policy and guidance to the retail industry. Unlike regulators in the safety domain, there is no defined responsibility at the regulator level to ensure organisations are compliant (Levinson, 2012); only to hold organisations accountable for "cyber-related misconduct" (Risen, 2014; Michaels, 2014).

Constructing Accident Causation

The STAMP analysis considers how hazardous control actions, mental model flaws, conflicting controllers and missing feedback within Target's security system migrated the system into a state of elevated risk, and created the conditions by which a cyber-attack would lead to a significant loss of private data. The analysis will be presented from a bottom-up approach which first addresses those individuals/groups who were directly involved in the cyber security first and then upward through the system hierarchy to management and regulatory bodies.

A hierarchical safety control structure diagram was produced (Figure 2) to depict Target's control structure for protection against POS attacks, and highlights the process failures that were considered to contribute to the breach –red lines and text indicate control flaws/degradations, and dotted grey lines indicate missing control processes. Four key components of the sociotechnical systems were identified for detailed analysis: i) the compromised vendor (Fazio), ii) Target's internal security team, iii) Target senior management and iv) the governmental/regulatory bodies overseeing information security for the US retail sector.

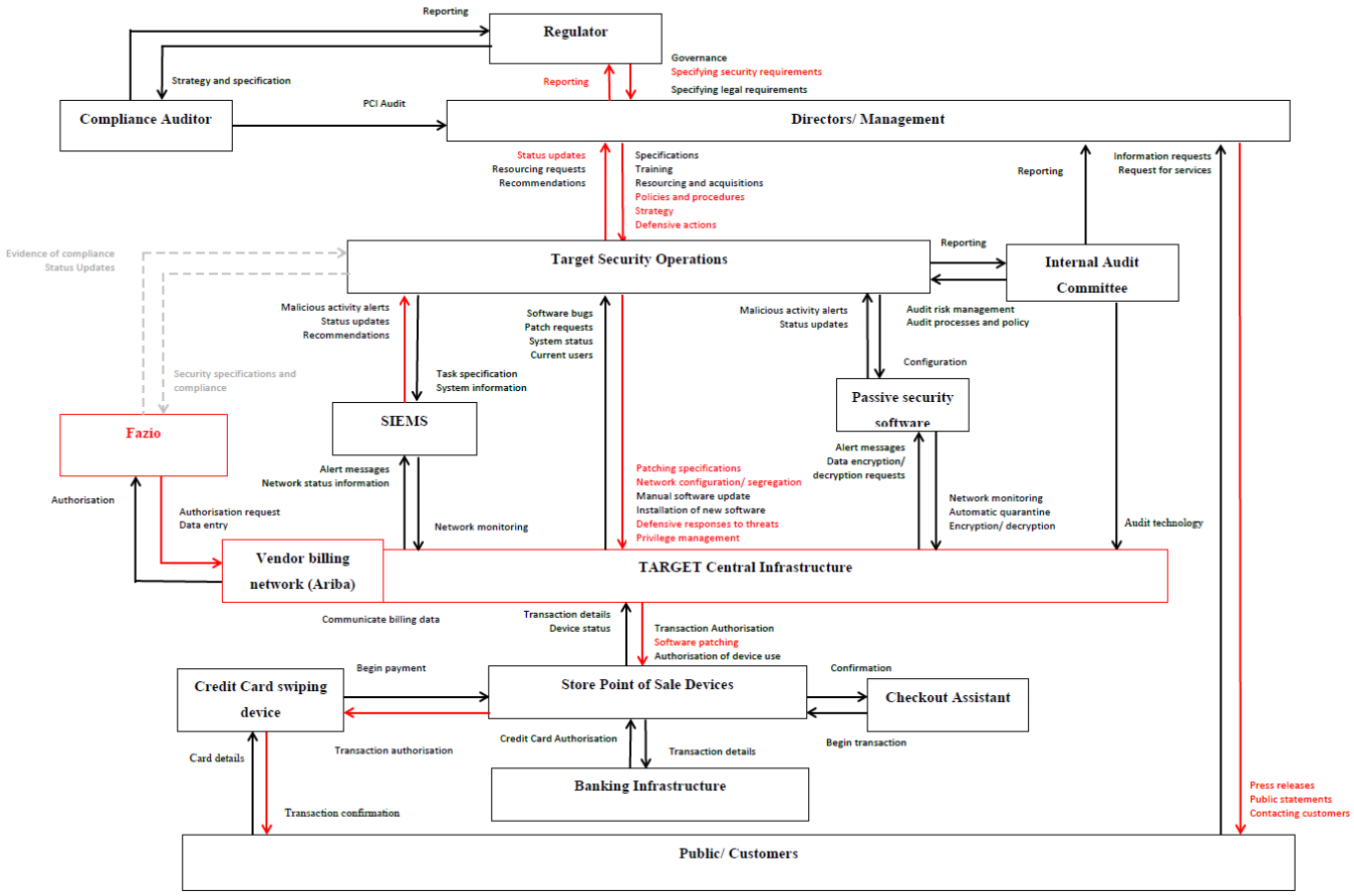

Figure 2 – Target Corporation Process Control Diagram for Information Security

i) Compromised vendor (Fazio) in the Supply Chain

Fazio were not considered to be any more or less secure than any other similarly-sized organisations within Target's supply chain. The attackers exploited human engineering techniques designed to elicit user credentials and passwords. However, evidence suggests that Fazio did not design and operate their security systems in harmony with Target Corporation, and vice versa. Whilst compliant with US regulations, Fazio were not operating to industry best practices, for example relying on free antivirus software. Interactions between Target and their supply chain were limited to business practices, and did not extend to information security, despite the prevailing issue that supply chains are often the most likely path through which attackers can access the networks of larger organisations. This flaw meant that security constraints on the system (see Constraint 1, above) could not be enforced by Target, who had little to no information on how their supply chain operated to protect their own data, and Target's data. In particular, human factors aspects such as training, awareness and internal security audits (based on a quality management system) would have decreased the likelihood of Fazio being compromised by social engineering techniques and could have been a positive approach to developing a security conscious organisational culture.

ii) Target Security + Point of Sale (POS)

The intended design of Target's security system was to isolate the vendor network from Target's central corporate network, and thus restrict supply chain accessibility to company information. This system was configured and controlled by Target's own internal security team, who were responsible for monitoring, testing and updating the networks, including network traffic.

However, security configuration flaws, such as default username and passwords and lack of 2-factor authentication allowed attackers to pivot from the vendor network onto the corporate network, using a combination of known and new exploits to leverage access onto the system. This may have indicated several system control flaws relating to verification of correct network configuration, testing of network security, and effective monitoring processes. There was little evidence to suggest that extensive and consistent verification and testing was conducted on security systems within Target due to the inconsistent network configuration, lack of 2-factor authentication and presence of 'default' usernames and passwords on the network. Furthermore, Target's monitoring systems, using a combination of automated SIEMS system and routine manual checking, failed to actively recognise and address suspicious activity on the network. Ultimately, there may not have been a clear (or at least comprehensive) conduct of operations for the security team, and certain key tasks were not procedurally led and therefore solely reliant on the competence of staff members to operate without adequate guidance and policy.

Where successful detection of the attack did occur (by the automated SIEMS) over a period of several months, the threat was not acted upon. A missing control loop within the system meant that feedback provided by the SIEMS to Target staff was not escalated through organisational channels to the appropriate individuals/team within Target with authority to initiate a response. This combination of inadequate network testing and monitoring activities created a latent condition which violated all system security constraints; where a successful breach of the vendor network allowed attackers to aggressively and quickly access the corporate network unchecked and subsequently hijack Target's POS patching service. This shortfall again appears to indicate inadequate policies within the organisation to provide a suitable chain of communication to raise and escalate security threats.

iii) Target Senior Management

Control of sensitive data was not suitably managed by Target – who allowed sensitive security data to be exported outside of their virtual perimeter onto the public domain, whereby it could be collected as part of an intelligence gathering campaign by attackers. As organisational data can be handled and controlled by multiple areas of an organisation, it is judged that the control flaws related to data control occurred due to inadequate control and enforcement of individuals who were responsible for marketing data and interactions with the public domain.

The failures of Target's security team to control and manage the corporate network lead to an exploration of potential control flaws by senior management, who are the controllers of the security team. The control flaws identified within the security team imply that an inadequate risk and vulnerability management program did not exist. The RAM scraping software did not present a new or novel attack vector, and Target should have been aware of the importance of POS security to protect against these threats. Furthermore, Target's security team had raised concerns with shortfalls in POS security but these were not acted upon by senior management (Radichel, 2014), demonstrating poor internal communication channels and conflicting allocation of responsibilities.

Senior management did not effectively perform their control actions on the security team, in terms of overall strategy and quality assurance processes, which likely impacted training, quality assurance, supply chain management, security policies and procedures. That the security team were not able to act upon POS security concerns with the kind of autonomous decision making normally given to a specialist team indicates that conflicting controllers may have existed within the organisation. Ambiguity in role allocation as a leading cause of accidents is well documented by Leplat (1987), and would have caused conflicts and inefficiencies to exist within the system.

iv) Regulatory Bodies

Unlike traditional causal analysis techniques and chain of event models, STAMP allows for an exploration of the entire sociotechnical system, including the influence of control actions performed by regulatory and auditing bodies and the impact these have on how Target operated their security system.

Target and Fazio were both compliant with Payment Card Industry (PCI) regulations, and considered that this indicated a strong information security system. This was a fundamentally flawed mindset, as it is not feasible for auditing to comprehensively assess all aspects of a security system; placing emphasis on organisations to establish a proactive security management system in addition to audits. Radichel places culpability of this mindset on Target senior management, and indeed some level of complacency may have existed within the management team that led to the wide range of control flaws identified throughout the organisation.

However, the STAMP analysis allows a further interpretation to be made, that places Target's own failing within a wider context and suggests that such behaviours and mindsets were widespread within the cyber security industry. Whilst somewhat speculative, this perspective is not without evidence. Through 2013-2014, a number of US retail organisations, including Target, were breached using almost identical attack vectors relying upon spear phishing, exploitation of widely known vulnerabilities and hijacking POS patching services to install RAM scraping software. The striking parallels between these attacks over the course of a single year suggests a failing within the approach to security taken by the US retail industry.

The security culture and mindset within a particular industry are heavily influenced by the governmental (e.g. regulatory) bodies that oversee it. The widespread breaches across the industry, and the mindset that compliance and certifications are a surrogate for security i.e. a 'compliance culture', have been inadvertently cultivated by the governmental bodies and were allowed to become pervasive in the industry. Understanding the extent to which regulators were culpable is a complicated matter. The United States does not assign responsibility for information security to a single organisational body, which is instead divided between federal agencies. Recommendations to improve industry wide communication, security culture and proactive security management therefore become more challenging to implement. This current arrangement of federal agencies may be one of the root causes as to why regulators and regulations have not been effective (a subject that warrants further research exploration).

Discussion

STAMP analysis has identified a number of critical systemic factors underlying the Target breach, namely inconsistent network security configuration, inadequate testing protocols, inadequate data control, and control flaws when transitioning from threat monitoring to escalation and response. The key human factors issues identified relate to staff training and awareness, security culture and conduct of operations – notably the lack of procedural guidance to support technical activities.

Whilst these findings are comparable to retrospective analyse by Radichel (2014), The US Senate Committee on Commerce, Science and Transportation (2005) and Shu et. al. (2017), STAMP has extending the analysis to stakeholders external to Target and has provided a more precise analysis of the specific mechanisms and control flaws that comprised the root causes of the accident.

Due to the limited information available on Target's management and security operations team, it is considered that there is still much to learn about the Target breach using the STAMP technique should more detailed information become available. However, even when analysis the system at a broad level, STAMP has been an effective causal analysis tool, that unlike other investigative reports not only highlights the high level design flaws and errors made by Target, but also the fundamental system flaws that should be corrected. As a technique, STAMP does not solely explore system flaws and incorporates human factors considerations and interactions with the systems. In the context of cybersecurity, it is important that systems are resilient to an evolving threat landscape. Security systems should not simply be designed to address 'known' threats but should be designed and controlled to adapt to new and unprecedented attack vectors. STAMP's ability to interrogate systems from a system's theory perspective, and consideration of the human element of the system, lends itself well to increasing resilient performance.

References

Besnard, D. and Arief, B., 2004. Computer security impaired by legitimate users. Computers & Security, 23(3), 253-264.

Bilge, L. and Dumitras, T., 2012. Before we knew it: an empirical study of zero-day attacks in the real world. In Proceedings of the 2012 ACM conference on Computer and communications security , ACM, 833-844.

Chen P., Desmet L., Huygens C., 2014. A Study on Advanced Persistent Threats. In: De Decker B., Zúquete A. (eds) Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science, vol 8735. Springer: Berlin.

Dhillon, G., & Backhouse, J., 2001. Current directions in IS security research: towards socio-organizational perspectives. Info Systems J11, 127-153.

Hauer, B., 2015. Data and information leakage prevention within the scope of information security. IEEE Access, 3, 2554-2565.

Hawkins, B., 2015. Case Study: The Home Depot Data Breach [online]. The SANS Institute. Viewed 22/11/2018. Available from: https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367

Hizver, J. and Chiueh, T.C., 2011. An introspection-based memory scraper attack against virtualized point of sale systems. In International Conference on Financial Cryptography and Data Security, Springer: Berlin, Heidelberg, 55-69.

Hong, J., 2012. The state of phishing attacks. Communications of the ACM, 55(1), 74-81.

Jarvis, K., and Milletary, J., 2014. Inside a Targeted Point-of-Sale Data Breach. Dell SecureWorks Counter Threat Unit Threat Intelligence [online]. Dell SecureWorks. Viewed 13/04/2018. Available from: https://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf

Kraemer, S., Carayon, P. and Clem, J., 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & security, 28(7), 509-520.

Kraemer, S. and Carayon, P., 2003. A human factors vulnerability evaluation method for computer and information security. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 47(12), 1389-1393. Sage CA: Los Angeles, CA: SAGE Publications.

Lee, M.G., 2012. Securing the human to protect the system: Human factors in cyber security. 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012, Edinburgh, 1 -5.

Leveson, N., 2004. A new accident model for engineering safer systems. Safety science, 42(4), pp.237-270.

Leveson, N., 2012. Engineering a safer world, system thinking applied to safety. Massachusetts Institute of Technology.

Michaels, D., 2014. SEC launches investigations of hacked firms [online].

The Boston Globe: Viewed 17/05/2018. Available from: https://www.bostonglobe.com/business/2014/07/02/hacked-companies-face-sec-scrutiny-over-disclosure-and-controls/rH1MlfdmqyKNHMu2yrusHP/story.html

Liginlal, D., Sim, I. and Khansa, L., 2009. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. Computers & security, 28(3-4), 215-228.

Radichel, T. 2014, Case Study: Critical Controls that Could Have Prevented Target Breach [online]. The SANS Institute. Viewed 28/03/2018. Available from: https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

Risen, T., 2014. FTC investigates Target data breach [online]. US News & World Report. Viewed 09/06/2018. Available from: http://www.usnews.com/news/articles/2014/03/26/ftcinvestigates-%20target-data-breach

Schwartz, M.J., 2013. Target breach: 10 facts [online]. Retrieved from Dark

Reading. Viewed 28/03/2018. Available from: http://www.darkreading.com/attacks-and-breaches/target-breach-10-facts/d/d-id/1113228

Shu, X., Tian, K. and Ciambrone, A., 2017. Breaking the target: an analysis of target data breach and lessons learned. arXiv preprint arXiv:1701.04940.

US Senate Committee on Commerce, Science and Transportation, 2005, A “Kill Chain” Analysis of the 2013 Target Data Breach. Majority Staff Report for Chairman Rockefeller.

Young, W.E., 2014. STPA-SEC for cyber security mission assurance. Eng Syst. Div. Syst. Eng. Res. Lab.

Young, W. and Leveson, N.G., 2014. An integrated approach to safety and security based on systems theory. Communications of the ACM, 57(2), 31-35.