




Situational Crime Prevention and the Mitigation of Cloud Computing Threats

Chaz Vidal¹ and Kim-Kwang Raymond Choo^{2,1} 

¹ School of Information Technology and Mathematical Sciences,
University of South Australia, Adelaide, SA 5095, Australia
raymond.choo@fulbrightmail.org

² Department of Information Systems and Cyber Security,
University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

Abstract. Security is a key challenge in the deployment and broader acceptance of cloud computing services, and existing research efforts include evaluating the effectiveness of various security solutions such as security policy implementations and technological solutions. Attacks on cloud environment may be considered from the criminological perspective, and crime theories be used to protect the cloud. This paper introduces a conceptual cloud security model utilizing the concept of situational crime prevention (SCP). Using SCP techniques, it may be possible to design process and technology-based steps to modifying the cloud computing environment to make it less attractive to crime.

Keywords: Situational crime prevention · Cloud security
Crime opportunity theories

1 Introduction

The use of cloud computing has become ubiquitous in recent years. Cloud computing comes in many forms such as easily configurable servers (e.g. those from Amazon Web Services and other cloud service providers) and online file storage services (e.g. Dropbox). Consumers with access to these technological resources then have the ability to use the resources in the way they need, such as building virtual servers for application development or web serving or online internet based backups. Most of these uses are generally non malicious, but with the use of technology does comes with it an inherent risk as overall security remains a prime concern certainly for cloud service providers (CSPs) and those who use cloud services.

Security is a major impediment to the overall uptake of cloud computing and there have been a number of security incidents that involved the use of cloud services in high profile criminal activities, which in turn highlights the need for enhanced security, privacy and forensic capabilities (Hiller and Russell 2013; Quick et al. 2013). Such incidents may also be considered cybercrime if they are in violation of existing legislation at the jurisdiction the incidents occurred or where the victim is located. Cloud computing infrastructure can then be protected using a combination of specific technology-based solutions (Vidal and Choo 2015; Osanaiye et al. 2016; Poh et al. 2017).

A large number of strategies to manage and enhance security within cloud computing environments have also been proposed in the literature (Ab Rahman and Choo 2015; Iqbal et al. 2016). However, we approach this from a different perspective. Specifically, we posit that a more effective approach is to combine existing mitigation strategies using the lens of a crime prevention theory, i.e. situational crime prevention (SCP) in this paper. In the next section, we present background information.

2 Cloud Security

Cloud computing has arguably come of age. It has progressed from a collection of web-based services to a clearly defined computing strategy, one that is used by both commercial consumers and large enterprise customers alike. The National Institute of Standards and Technology (NIST), for example, describes cloud computing as a model for enabling network access to configurable computing resources quickly with minimal interaction from own service providers (Mell and Grance 2011).

NIST also ascribes five characteristics of a cloud service model, namely: on-demand self-service, seamless network access, resource pooling, rapid elasticity and measured services. The service models include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In recent times, other service models have also been suggested in the literature such as Security as a Service (Varadharajan and Tupakula 2014), Collaboration-as-a-Service and Network-as-a-Service (Gu et al. 2013).

NIST further defines how these service models are deployed, namely: a private cloud, a community cloud, a public cloud or a hybrid cloud.

The technology for cloud computing has matured and have become widely accepted (Khan et al. 2012). However, despite these improvements, there are difficulties that have been recognized as barriers to wider acceptance. One particular aspect of cloud computing that has become more problematic is ensuring adequate security is implemented both for its potential users and by CSPs (Lokhande and Shelke 2013).

Despite its maturity, cloud computing is still vulnerable to security issues including cyber attacks and misuse and abuse of the cloud computing infrastructure. Some of these attacks are more difficult to carry out in nature such as extracting private information from different virtual machines (VMs) that share the same cloud computing resources. Other attacks are more traditional such as Distributed Denial of Service (DDoS) on known public clouds (Dawoud et al. 2010). Cloud computing is also vulnerable to misuse and abuse from its own users such as using cloud resources to host malware or contraband or illegal material (Choo 2010; Julidotter and Choo 2015; Rogers 2012).

Because of the potential for misuse by the criminal element, the onus not only is on the cloud users to protect and educate themselves on cloud usage but also on CSPs to establish protection mechanisms (Antonopoulos and Gillam 2010).

For CSPs, a number of strategies can be employed to ensure that adequate protection of the cloud service. As an organization, CSPs can apply Information Security standards to their services (AS/NZS 2006; Ab Rahman and Choo 2015). These standards will allow the CSPs to identify the threats and risks associated with the delivery of the cloud service and formulate specific controls to mitigate these risks.

Identifying cloud computing risks have been an easier job for CSPs because of the availability of industry-based groups and their work in showing the top threats to cloud computing. The Cloud Security Alliance, for example, over the past few years have shown where CSPs should concentrate on to mitigate the threats to their cloud services (Cloud Security Alliance 2016).

3 Cybercrime in the Cloud

Since the advent of computers and their availability for most everyone, cybercrime has been steadily on the rise. There have been several attempts to describe cybercrime and there appears to be some difficulty in providing a universally accepted definition (Hunton 2011). In recent years, cybercrime has been used to describe technology related criminal acts perpetrated through the Internet but at the same time, there are instances when cybercrime covers more than just criminal acts but also includes undesirable or offensive behavior.

With the many definitions in use today, it is important to focus on an agreed to framework to describe cybercrime and cyber-criminals. Australia's National Cyber-crime Working Group working under Australia's Attorney-General Department (2013) produced a definition to cybercrime which describes cybercrime in two aspects:

- Crimes directed at computers or other information communications technologies (ICTs) (such as hacking and denial of service attacks), and
- Crimes where computers or ICTs are an integral part of an offence (such as online fraud, identity theft and the distribution of child exploitation material).

The first point describes crime that is targeted directly at networked and computer environments which cloud computing infrastructure is inherently based on. The second one describes the commission of traditional physical crimes utilizing the available technology today which indicates illegal usage of cloud computing resources can very well be classified as cybercrime.

These types of activities over the past few years have escalated and we can show how business has suffered. In 2013, for example, the InfoSec Institute (Paganini 2013) gathered existing research on the costs of cybercrime and showed that this was rising. In the United States alone, each cybercrime incident costs on average \$12 million which was up over 78% from 4 years ago.

Verizon (2015) published a report on data breaches from cybercrime episodes and the underlying cause and overall cost of such data breaches. They came up with a cost per record model, which indicated how much a set of records stolen from organizations could be used and monetized for fraud. The cost goes up from as low as \$392,000 to \$200 million with an expected average of \$8.8 million per 100 million records lost through data breaches.

For small business, the impact of cybercrime can also be felt. Industry security organizations like TrendLabs (2015) reported that even the smallest of business can fall prey to cybercriminals simply because these businesses also store information that these criminals need and want. Personal identification information such as addresses, social security numbers and banking account numbers and security PINs and credit

card numbers are still stored by these small business and are an attractive target for determined attackers. With a larger percentage of small business moving to the cloud, cybercriminals are sure to follow suit.

A survey performed by the consulting firm PricewaterhouseCoopers (PwC) in cooperation with the United States Computer Emergency Response Team (US-CERT) and the US Secret Service in 2014 on US business reported that 34% of respondents showed an increase in cyber security incidents year on year (PWC 2014). Self reported losses were approximately \$415,000 on average and these were caused by cybercrime activities such as malware, phishing, network interruption, spyware, and denial of service attacks. In many cases, businesses point the blame at attackers from outside the organization. However, there was still a large percentage that pointed to malicious insiders as the cause of a number of security incidents.

In Australia, the problem of cyber security is not just confined to large business but small businesses are especially vulnerable. This is not surprising, as small businesses may find the use of cloud computing particularly cost effective and allow them to compete with larger enterprises on a level playing field. The use of cloud computing too has become the focus of a determined criminal element. While there have been fewer attacks against CSPs, there are still risks associated with the use of cloud computing, such as the following:

- Authentication Issues that could be exploited to allow access to data by unauthorized personnel (Abdollahifar 2013).
- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks that will cause clients to lose access to required services (Archer and Boehm 2009).
- The coopting of cloud services for criminal activities such as utilizing cloud resources to run malware and botnet networks (Osaniye et al. 2016; Ouedraogo and Mouratidis 2013).
- CSPs complicit in criminal activity such as allowing the storage of copyrighted material (Duncan et al. 2012).
- Physical attacks on data centers containing cloud computing infrastructure and other insider activities can cause data breaches are lead to illegal remote access to data (Greenberg et al. 2008).
- Data stored in the cloud could also be vulnerable through vulnerabilities, say in software components (e.g. flawed implementation of encryption), or external attacks via phishing and man in the middle attacks (Hooper et al. 2013).
- Other attacks also involve skipping attacks on the cloud infrastructure itself and targets the client devices used to access the network resource such as compromising the client access via key loggers or web session hijacking (Ghorbani et al. 2010), or seeking to circumvent security solutions (e.g. SSL/TLS validations) on client devices (D'Orazio and Choo 2017; D'Orazio et al. 2017).

4 Cybercrime and Situational Crime Prevention

More and more business are looking to use cloud computing to gain competitive advantages and to cut costs in delivering their own services. Consumers are also in the same path to using cloud computing resources for different reasons, such as ease of use and the availability of computing resources for a fraction of the cost of buying it themselves. Because of this, cyber criminals are attempting to exploit cloud computing weaknesses to reach their targets, which can be for financial gains, to gain competitive advantages, for national security related matters (e.g. by state-sponsored actors), or illegal content (Paganini 2013).

Examples of attacks on cloud based services include:

1. DDoS based attacks against cloud services such as the Xbox and Playstation networks (Sawers 2015).
2. DNS based attacks that caused access problems to IaaS provider Rackspace (O'Connor 2014).
3. Hijacking of existing IaaS servers provided by Amazon for BitCoin mining processes (Litke and Stewart 2014).

Reports suggest that the number of incidences of cybercrime, especially against cloud services is poised to rise (PWC 2014). More recently in 2017, Microsoft (2017) reported that:

the frequency and sophistication of attacks on cloud-based accounts are accelerating. The Identity Security and Protection team has seen a 300 percent increase in user accounts attacked over the past year. A large majority of these compromises are the result of weak, guessable passwords and poor password management, followed by targeted phishing attacks and breaches of third-party services (Microsoft 2017, p. 3)

As such, it would be beneficial to understand how these crimes can occur. One way to begin understanding the roots of these types of crimes is to use crime science. Crime science seeks to explain how crime transpires (Hartel et al. 2010). This is somewhat different from criminology that seeks to frame the crime in terms of the criminal's behaviors and motivations. Crime science utilizes conceptual frameworks to explain the actual incidents of crime, the "how" if you will, and not the actual criminal; or the "who" and "why". In this manner, crime science is a problem solving approach to crime that is outcome specific.

One such approach in use in crime science is the crime opportunity theory which, at its core, suggests that opportunity "plays a role in all crime" (Felson and Clarke 1998). Felson and Clarke's (1998) research was the basis of formulating this approach, which was a departure from the prevailing theories of crime at the time which focused on the reducing criminal propensities instead of reducing opportunities for crime.

There are three main aspects to the crime opportunity theory. The first is called the Routine Activity Theory (RAT), which tries to frame that crime is more likely to occur when there is the occurrence of three aspects which are a possible criminal or offender, a likely or highly valued target and the absence of a capable guardian against the crime to act.

The second is the Crime Pattern Theory (CPT), which makes the case for how criminals and targets are located at any given time. Using three main concepts, namely: nodes, paths and edges, this theory attempts to describe crime in a way that suggests movements.

- Nodes designate where people or targets come and go.
- Paths between nodes indicate how and where people travel.
- Edges refer to areas where people congregated to live, work or enjoy recreation.

CPT uses these concepts to map out likely incidences of crime within these areas.

The third is the Rational Choice Theory and it introduces the concept that criminals make very specific and, to their own mind, rational and logical choices when enacting a crime. This theory tries to frame how a criminal offender makes choices when enacting short-term criminal goals and in so doing, tries to understand how the criminal choice occurs within a particular motive and specific opportunities.

Taken together, these aspects frame crime as occurring in many levels. From the larger level of society; which the Routine Activity describes, to the local area which CPT maps out; to the individual criminal, whose actions are governed by rational choice. Ensuring that opportunities for crime are reduced at all these levels changes the instances of crime.

These theories then are used to structure a preventative approach to crime – situational crime prevention (Clarke 1997) as well as a refinement to this initial approach (Cornish and Clarke 2003). This approach to crime prevention introduces specific changes in the management and environment where a crime occurs. Clarke (1997) describes situational prevention to include three aspects to reduce the opportunities for crime. That it is directed at highly specific forms of crime, involve the management of the environment of the crime and making the commission of the crime itself less rewarding and more risky and difficult as well as less excusable for offenders.

Clarke then showed SCP procedures and case studies in which such procedures were utilized and explained that “[s]ituational crime prevention then involves the development of techniques to prevent, constrain or disrupt criminal activity” (Clarke 1997).

In another approach to crime prevention, Cornish (1994) used concepts from the Rational Choice Theory to propose an approach to preventing crime through disrupting an offenders approach to crime, their “crime script” and ensuring that this natural flow of the crime is interrupted at various points. He posited that crime follows a series of steps or that criminals follow a “script” of some kind such that crimes occur according to this script. If this crime script is disrupted at any point, then there is to be the expected change in the behavior and the prevention of the crime itself. This was demonstrated in research performed by Smith (2014) that showed how disrupting the natural flow of a recruitment process for criminal organizations aids in the minimization of criminal behavior.

Using concepts of RAT, it is also suggested that modifying any of the three aspects (motivated offender, suitable target, and capable guardianship) can prevent crime. Hollis-Peel and Welsh (2014) tested this theory to show how guardianship can be measured and used to prevent crime in maintaining home security.

Utilizing the crime opportunity theories and SCP, various research has been made to adapt these theories to cybercrime in general and specific cybercrime in particular.

Although created and developed primarily for physical crimes, the crime opportunity theories and their associated aspects have been adapted to understand the incidence of cybercrime.

When it comes to cyber security and the mitigation of threats against computing infrastructure, so called cyber threats, solutions have either come from a technological or a process or policy specific area. These security solutions concentrate on identifying and mitigating these cyber threats through employing security controls such as employing new processes (Goodman et al. 2008), or using technology to mitigate identified weaknesses in infrastructure (Christie 2011). A holistic way to prevent cybercrime specifically or crime in general is to employ SCP models.

SCP is a technique that has emerged from the crime opportunity theories co-developed by Clarke (1983). Clarke says that in order to reduce crime, there must be changes to the environment of a crime to reduce the opportunities for a crime to occur and that “the pivotal point of situational crime prevention theory is that the criminal’s pseudo-rational decision is a function of the perceived net benefits. If crime prevention measures do not adequately increase perceived costs and decreased perceived benefits, rational choice theory argues that the crime will not occur” (Clarke 1997).

Some research suggests that cybercrime is a different category of crime and that these crimes cannot be easily explained by the prevailing crime theories (Yar 2005). However, other research, such as from Beebe and Rao (2005), have taken the SCP theories and extend them to apply to the growing problem of information system security. In their research, they used SCP techniques and suggested a theoretical model that can be applied to an online environment (Beebe and Rao 2005). They suggested that in the model to look at the reduction of anticipated benefits for cybercriminals in engaging in cybercrime although they did not offer any concrete steps or activities to reducing these benefits.

Other aspects of crime opportunity theory have also been used to map into specific cases of cybercrime. Pratt et al. (2010) showed how RAT can be used to model the incidence of internet fraud. He showed that the change in consumers’ behavior, especially in the use of online shopping, exposes them to motivated offenders attempting to perpetrate consumer fraud. As such, SCP plays a role in understanding that will be more likely to be targeted in cases of Internet fraud and what they can do to protect themselves. Pratt’s research showed that RAT could be used as a general framework in so much as preventing a very specific case for cybercriminal victimization.

Leukfeldt (2014) did a similar study on phishing attempts which came up with some differing results. Using RAT as a basis, the study attempted to find out if phishing victimization rates were higher in any particular demographic (target) but showed that increasing capable guardianship via target hardening may help. Overall the study showed little effect of changing the circumstances for RAT based approach to crime prevention and suggested that other aspects of SCP should be used.

Although research has been done on the effects of cybercrime on individuals, RAT has also been used to show how highly connected countries have a higher incidence of cybercrime, specifically the incidence of spam and phishing attempts (Kigerl 2012).

This goes to show that more the opportunities for crime are higher in more connected countries.

Navarro (2013) used RAT to map out another aspect of cybercrime, that of cyber bullying or harassment. It showed how RAT fits into explaining the incidences of cyber bullying victimization when a lack of capable guardianship, one of the three conditions for crime to occur, according to the RAT, is present in the online activities of teenagers. Their results at applying the crime opportunity framework were mixed at best because of the way their research was structured around gender lines.

Hinduja and Kooi (2013) utilized general aspects of SCP to address a framework for reducing information security vulnerabilities. They posited that technological solutions are not enough to address vulnerabilities in information systems and that SCP can be used to combat the more opportunistic elements of cybercrime. In their paper, they only considered using Clarke's original 16 opportunity reducing techniques instead of the latter 25 primarily because they determine some of the newer techniques not to be relevant to information security, such as the reduction of provocations due to drugs and alcohol (Hinduja and Kooi 2013).

Similarly, Willison and Backhouse (2006) extended the concepts of SCP to increasing IS security, utilizing the same methods and additional crime theory frameworks. The authors combined the crime script theory with classic SCP techniques and mapped it into potential IS security policies or activities, and specifically on the common cyber security concept of insider threats and how SCP in coordination with IS security policies can be used to mitigate these threats. Willison (2000) also put forward his conceptual Crime Specific Opportunity Structure as a means to understand the circumstances behind information systems risk and to help elaborate the relationships that offenders have with the environment of the crime.

After reviewing the available research on crime opportunity theory and its subsequent SCP applications, it is clear that SCP can be applied to the protection of many aspects of information systems. Although there are SCP techniques for specific threats such as fraud (Samonas 2013) and malicious insiders (Stockman 2014), there does not appear to be an overarching framework that can be applied to protecting cloud computing infrastructure and services. This is a challenge because SCP, according to Clarke (1997), applies to very specific forms of crime and actions against cloud computing can be varied and wide ranging. This suggests different techniques for every threat against cloud computing.

Existing information security frameworks have tended to work on two levels (i.e. technological and process) to mitigate threats. Examples of technological framework solutions include those of Takabi et al. (2010) and Brock and Goscinski (2010), where they break down the cloud infrastructure architecture components and introduce conceptual modules that contain technological solutions to protect each component. In one example, interfaces between cloud users and CSPs can be protected via an access control module that can conceptually contain Role-Based Access (RBAC) control models, such as those proposed by Alam et al. (2017).

The Australian Signals Directorate (2017) has also published specific strategies to combat cybercrime that can be implemented by cloud consumers and CSPs. Strategies such as regular software patching and restricting administrator privileges are practical activities that can be implemented to protect against cyber intrusions. These technology

strategies can be made to apply generically across computing infrastructure including cloud computing platforms.

Cyber security can also be driven from a policy perspective as well. NIST has published standards that seek to increase the overall security of information systems through policy controls that map out key information security factors such as security governance, systems development lifecycle, systems acquisitions, systems interconnections, ongoing performance metrics, planning and security incident responses among others (Bowen et al. 2006; NIST 2017; Stoneburner et al. 2001). The International Standards Organization (ISO) has also published information security standards, which is a series of security controls that organizations can implement to increase security. Foremost of these controls is the establishment of security policy. The security policy is meant to contain the organization's security goals and what roles and responsibilities each member of the organization is meant to have. Having an established security policy is the first step to ensuring that information assets are protected, risks are minimized and that organizations are compliant to regulations (AS/NZS 2006).

Given the relationship of cloud computing platforms and the digital information contained therein, the application of information security policies onto cloud computing implementations can be of great benefit and some research has already been undertaken to look at increasing security through this method. For example, Carrol et al. (2011) took the approach of applying specific security policies to a cloud computing scenario where certain elements of the NIST and ISO standards have been used to mitigate risks the authors have identified as applicable to cloud computing services.

After the technological and policy driven solutions for cloud security, we can introduce the third concept of SCP. There has been research that shows SCP to be potentially useful in protecting against specific cybercrime instances. However, there is a possibility that the application for SCP techniques can be used for protection of cloud computing systems.

Choo (2014) has put forward a conceptual framework to mitigate cyber security threats with the use of different crime theories and crime prevention strategies can be "plug and played" into so that a wider ranging plan can be enacted. The framework proposed is to be applicable to a generalized information security model and utilizes various disciplines in order to consolidate the relationships between different objects or actors in an information security context. This means that because there are various objects in play in a cyber security activity (e.g. people, process, and technology), and a recognition that there are different schools of thought as to how and why these incidents occur. It is of use to have a framework where various theories can be used to understand the existing environment and therefore mitigate the ensuing cyber security risks. The author then uses as an example using SCP techniques to understand the cyber security environment and to look at modifying the environment to combat crime.

So far, there has been a number of technological and policy driven approaches to increasing information security. There has also been support for SCP approaches for very specific cybercrime instances. Thus, we posit that using SCP techniques that apply and involve increasing perceived effort and risks of committing the crime, reducing rewards and provocations and removing excuses for the criminals could lead to a reduction in criminal actions against cloud computing services. Specifically, we present

a conceptual framework of mitigation of cloud security threats utilizing a combination of these approaches.

The next section will describe this conceptual framework and how this can be applied to cloud computing services.

5 A Conceptual SCP Model for Cloud Security

There are a variety of solutions intended to tackle the problem of cybercrime and cyber security. Because several policy-based solutions are available from different standards bodies, it is important to choose one set of solutions to enact. Controls from the AS/NZS ISO/IEC Standard 27002:2006 (Security Techniques) as the basis for the initial policy solutions, as this provides us with a comprehensive security solution that can be applied to a wide number of information systems including cloud computing platforms.

There are a number of controls available within the ISO Standard; therefore, it is necessary to create designations for each control that could be applied to a cloud computing solution (see Table 1).

Table 1. Policy controls solutions

Security control	Designation
Establishment of a security policy	P1
Organization of information security	P2
Asset management	P3
Human resources security management	P4
Physical and environmental security	P5
Communications and operations management	P6
Establish operational procedures and responsibilities	P7
Third-party service delivery management	P9
Malicious/mobile code	P10
Backup	P11
Network security management	P12
Media handling	P13
Information exchange	P14
Electronic commerce service	P15
Monitoring	P16
Access control	P17
Information systems acquisition, development and maintenance	P18
Information security incident management	P19
Business continuity management	P20
Compliance management	P21

These policy and technology based solutions can be applied to specific cloud threats in the proposed conceptual model. If the conceptual model is implemented by a CSP, then it may be possible to measure the effectiveness of the changes in mitigating these threats to the environment.

According to Clarke (1997), SCP consists of three different measures:

1. Measures directed at highly specific forms of crime.
2. Involves changes to the environment where crime occurs.
3. Strives to make crime less rewarding, more risky and less excusable for offenders.

Because of these measures, it is important for the conceptual model to take into account the risks associated with a cloud computing infrastructure and to modify this particular environment so that criminal activity is discouraged. This model then starts with industry identified threats and vulnerabilities against cloud computing as a source of crime that can be countered or mitigated.

SCP techniques are then applied to each of these threats in order to lower the risk and incidence of these vulnerabilities being exploited, to alter the environment in a way.

With each set of techniques, both technology based and policy based solutions are then invoked to enable the changes in the cloud computing environment. These changes, as directed by SCP, will then be expected to discourage the commission of these crimes. The expected result in turn could lead to increased security for the entire cloud computing environment.

To identify the cloud computing threats that this framework can be applied this paper turns to the major risks identified by the industry via the Cloud Security Alliance, which published their top nine threats to cloud computing (Cloud Security Alliance 2016). Utilizing the top threats in this conceptual model of cloud security and to target each as a specific form of crime, solutions can then be applied so as to change the cloud computing environment and decrease the overall opportunities for crime. Technology and process solutions from standards organizations and governmental authorities such as the ISO 27002 standard and the Australian Signals Directorate (2017) – see also Table 2 – can then be used to change the environment for each threat as a means of mitigation.

Each solution is expected to enact changes in the environment to increase effort, increase risk, decrease reward, remove provocations and remove excuses within the environment. This relates back to the SCP strategies for reducing crime.

The solutions that may be applied could be very specific to the cloud computing components, such as the virtualization infrastructure, or it could be generalized as well, such as to the entire cloud computing organization depending on the set of remediation strategies to use. In Table 3, we can see potential solutions being assigned to cloud threats. The targeted outcomes should still be the same: a change of the environment to lower crime opportunities.

Utilizing this model, we can then start to build the framework by combining various mitigation solutions across the different threats and understanding their effect on modifying the cloud computing environment.

Table 2. ASD mitigation strategies

Mitigation strategy	Designation
Application whitelisting of permitted/trusted programs	A1
Patch applications e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office	A2
Patch operating system vulnerabilities	A3
Restrict administrative privileges to operating systems and applications based on user duties	A4
User application configuration hardening and disabling of vulnerable plugins	A5
Automated dynamic analysis of email and web content run in a sandbox to detect suspicious behavior	A6
Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) and Enhanced Mitigation Experience Toolkit (EMET)	A7
Host-based intrusion detection/prevention system to identify anomalous behavior during program execution	A8
Disable local administrator accounts	A9
Network segmentation and segregation into security zones	A10
Multi-factor authentication especially implemented for remote access, privileged actions or sensitive information access	A11
Software-based application firewall, blocking incoming network traffic	A12
Software-based application firewall, blocking outgoing network traffic	A13
Non-persistent virtualized sandboxed trusted operating environment	A14
Centralized and time-synchronized logging of computer events	A15
Centralized and time-synchronized logging of allowed and blocked network activity	A16
Email content filtering, allowing only whitelisted business related attachment types	A17
Web content filtering of incoming and outgoing traffic	A18
Web domain whitelisting for all domains	A19
Block spoofed emails using Sender ID or Sender Policy Framework (SPF)	A20
Workstation and server configuration management based on a hardened standard operating environment	A21
Antivirus software using heuristics and automated Internet-based reputation ratings	A22
Deny direct Internet access from workstations by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or web proxy server	A23
Server application configuration hardening	A24
Enforce a strong passphrase policy	A25
Removable and portable media control as part of a data loss prevention strategy	A26
Restrict access to Server Message Block (SMB) and NetBIOS services	A27
User education	A28
Workstation inspection of Microsoft Office files for malicious abnormalities	A29
Signature-based antivirus software that primarily relies on up to date signatures to identify malware	A30
TLS encryption between email servers and perform content scanning after email traffic is decrypted	A31
Block attempts to access websites by their IP address instead of by their domain	A32
Network-based intrusion detection/prevention system using signatures and heuristics	A33
Gateway blacklisting to block access to known malicious domains and IP addresses	A34
Capture network traffic to/from internal critical asset workstations and servers	A35

Table 3. Mapping of cloud threats and mitigation solutions with the SCP-based model

Cloud threat	Increase effort	Increase risk	Decrease reward	Remove provocations	Remove excuses
Data breaches	<i>P5, A2, A4</i>	<i>P4, P16, A33</i>	<i>P3, A14, A24</i>	<i>P1, P21, A28</i>	<i>P1, A1, A28</i>
Data loss
Account or service traffic hijacking
Insecure interfaces
Denial of service
Malicious insiders
Abuse of cloud services
Insufficient due diligence
Shared technology vulnerabilities

There is potential future work and research to develop this framework further by applying it to an existing CSP and observing the changes that this framework brings to the environment in terms of lowering crime opportunities.

References

Ab Rahman, N.H., Choo, K.-K.R.: A survey of information security incident handling in the cloud. *Comput. Secur.* **49**, 45–69 (2015)

Abdollahifar, A.: *Network and Security Challenges in Cloud Computing Infrastructure as a Service Model* (2013)

Alam, Q., Malik, S.U.R., Akhunzada, A., Choo, K.-K.R., Tabbasum, S., Alam, M.: A cross tenant access control (CTAC) model for cloud computing: formal specification and verification. *IEEE Trans. Inf. Forensics Secur.* **12**(6), 1259–1268 (2017)

Antonopoulos, N., Gillam, L.: *Cloud Computing: Principles, Systems and Applications*. Springer, Heidelberg (2010). <https://doi.org/10.1007/978-1-84996-241-4>

Archer, J., Boehm, A.: *Security guidance for critical areas of focus in cloud computing*. Cloud Security Alliance (2009)

AS/NZS: *ISO/IEC 27002:2006 - Information Technology - Security Techniques - Code of Practice for Information Security Management* (2006)

Attorney-General’s Department: *National Plan to Combat Cybercrime*. Attorney-General’s Department, Canberra, ACT, Australia (2013)

Australian Signals Directorate: *Strategies to Mitigate Cyber Security Incidents*. Australian Department of Defense, Canberra (2017)

Beebe, N.L., Rao, V.S.: Using situational crime prevention theory to explain the effectiveness of information systems security. In: *Proceedings of the 2005 Software Conference, Las Vegas* (2005)

Bowen, P., Hash, J., Wilson, M.: SP 800-100. *Information Security Handbook: A Guide for Managers* (2006). <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf>. Accessed 26 Mar 2018

- Brock, M., Goscinski, A.: Toward a framework for cloud security. In: Hsu, C.-H., Yang, Laurence T., Park, J.H., Yeo, S.-S. (eds.) ICA3PP 2010. LNCS, vol. 6082, pp. 254–263. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13136-3_26
- Carroll, M., Van Der Merwe, A., Kotze, P.: Secure cloud computing: benefits, risks and controls. In: Information Security South Africa (ISSA), pp. 1–9. IEEE (2011)
- Choo, K.-K.R.: Cloud Computing Challenges and Future Directions. Australian Institute of Criminology, Canberra (2010)
- Choo, K.-K.R.: A conceptual interdisciplinary plug-and-play cyber security framework. In: Kaur, H., Tao, X. (eds.) ICTs and the Millennium Development Goals, pp. 81–99. Springer, Boston (2014). https://doi.org/10.1007/978-1-4899-7439-6_6
- Christie, S.: 2011 CWE/SANS Top 25 Most Dangerous Software Errors (2011). <http://cwe.mitre.org/top25/>. Accessed 5 Sept 2013
- Clarke, R.: Situational Crime Prevention. Criminal Justice Press, Monsey (1997)
- Clarke, R.V.: Situational crime prevention: its theoretical basis and practical scope. *Crime Justice* **4**, 225–256 (1983)
- Cloud Security Alliance: ‘The Treacherous Twelve’ Cloud Computing Top Threats in 2016. Cloud Security Alliance (2016)
- Cornish, D.B.: The procedural analysis of offending and its relevance for situational prevention. *Crime Prev. Stud.* **3**, 151–196 (1994)
- Cornish, D.B., Clarke, R.V.: Opportunities, precipitators and criminal decisions: a reply to Wortley’s critique of situational crime prevention. *Crime Prev. Stud.* **16**, 41–96 (2003)
- D’Orazio, C.J., Choo, K.-K.R.: A technique to circumvent SSL/TLS validations on iOS devices. *Future Gener. Comput. Syst.* **74**, 366–374 (2017)
- D’Orazio, C.J., Choo, K.-K.R., Yang, L.T.: Data exfiltration from internet of things devices: iOS devices as case studies. *IEEE Internet Things J.* **4**(2), 524–535 (2017)
- Dawoud, W., Takouna, I., Meinel, C.: Infrastructure as a service security: challenges and solutions. In: 2010 The 7th International Conference on Informatics and Systems (INFOS), pp. 1–8. IEEE (2010)
- Duncan, A.J., Creese, S., Goldsmith, M.: Insider attacks in cloud computing. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 857–862. IEEE (2012)
- Felson, M., Clarke, R.V.G.: Opportunity Makes the Thief: Practical Theory for Crime Prevention. Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, London (1998)
- Ghorbani, A.A., Lu, W., Tavallae, M.: Network Attacks, 1st edn. Springer, Boston (2010)
- Goodman, S., Straub, D.W., Baskerville, R., Goodman, S.E., Ebrary, I.: Information Security: Policy, Processes and Practices. M. E. Sharpe Incorporated, Armonk (2008)
- Greenberg, A., Hamilton, J., Maltz, D.A., Patel, P.: The cost of a cloud: research problems in data center networks. *ACM SIGCOMM Comput. Commun. Rev.* **39**(1), 68–73 (2008)
- Gu, L., Zeng, D., Guo, D.: Vehicular cloud computing: a survey. In: IEEE Globecom Workshops, pp. 403–407 (2013)
- Hartel, P., Junger, M., Wieringa, R.: Cyber-crime Science = Crime Science + Information Security (2010). <https://research.utwente.nl/en/publications/cyber-crime-science-crime-science-information-security>. Accessed 29 Aug 2017
- Hiller, J.S., Russell, R.S.: The challenge and imperative of private sector cybersecurity: an international comparison. *Comput. Law Secur. Rev.* **29**(3), 236–245 (2013)
- Hinduja, S., Kooi, B.: Curtailing cyber and information security vulnerabilities through situational crime prevention. *Secur. J.* **26**(4), 383–402 (2013)
- Hollis-Peel, M.E., Welsh, B.C.: What makes a guardian capable? A test of guardianship in action. *Secur. J.* **27**(3), 320–337 (2014)

- Hooper, C., Martini, B., Choo, K.-K.R.: Cloud computing and its implications for cybercrime investigations in Australia. *Comput. Law Secur. Rev.* **29**(2), 152–163 (2013)
- Hunton, P.: The stages of cybercrime investigations: bridging the gap between technology examination and law enforcement investigation. *Comput. Law Secur. Rev.* **27**(1), 61–67 (2011)
- Iqbal, S., Kiah, M.L.M., Dhaghghi, B., Hussain, M., Khan, S., Khan, M.K., Choo, K.-K.R.: On cloud security attacks: a taxonomy and intrusion detection and prevention as a service. *J. Netw. Comput. Appl.* **74**, 98–120 (2016)
- Julidotter, N., Choo, K.-K.R.: CATRA: conceptual cloud attack taxonomy and risk assessment framework. In: Ko, R., Choo, K.-K.R. (ed.) *Cloud Security Ecosystem*. Syngress, an Imprint of Elsevier, Amsterdam (2015)
- Khan, M.F., Ullah, M.A., Aziz-Ur-Rehman: An approach towards customized multi-tenancy. *Int. J. Mod. Educ. Comput. Sci.* **4**(9), 39 (2012)
- Kigerl, A.: Routine activity theory and the determinants of high cybercrime countries. *Soc. Sci. Comput. Rev.* **30**(4), 470–486 (2012)
- Leukfeldt, E.R.: Phishing for suitable targets in the Netherlands: routine activity theory and phishing victimization. *Cyberpsychology Behav. Soc. Netw.* **17**(8), 551–555 (2014)
- Litke, P., Stewart, J.: BGP Hijacking for Cryptocurrency Profit (2014). <http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/>
- Lokhande, M.T.S., Shelke, P.R.R.: A review paper on cloud computing security. *Int. J. Adv. Res. Comput. Sci.* **4**(6), 70 (2013)
- Mell, P., Grance, T.: The NIST Definition of Cloud Computing (2011). <http://dx.doi.org/10.6028/NIST.SP.800-145>. Accessed 29 Aug 2017
- Microsoft 2017: Microsoft Security Intelligence Report, vol. 22, January–March 2017. http://download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security_Intelligence_Report_Volume_22.pdf. Accessed 29 Aug 2017
- National Institute of Standards and Technology (NIST): Security and Privacy Controls for Information Systems and Organizations (2017). <http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf>. Accessed 29 Aug 2017
- Navarro, J.N., Jasinski, J.L.: Why girls? Using routine activities theory to predict cyberbullying experiences between girls and boys. *Women Crim. Justice* **23**(4), 286–303 (2013)
- O'Connor, F.: Rackspace DNS Recovers After DDoS Brings System Down. In: *PCWorld* (2014). <http://www.pcworld.com/article/2863592/rackspace-dns-recovers-after-ddos-brings-system-down.html>. Accessed 29 Aug 2017
- Osaniye, O., Choo, K.-K.R., Dlodlo, M.: Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud ddos mitigation framework. *J. Netw. Comput. Appl.* **67**, 147–165 (2016)
- Ouedraogo, M., Mouratidis, H.: Selecting a cloud service provider in the age of cybercrime. *Comput. Secur.* **38**, 3–13 (2013)
- Paganini, P.: 2013 - The Impact of Cybercrime (2013). <http://resources.infosecinstitute.com/2013-impact-cybercrime/>. Accessed 29 Aug 2017
- Pratt, T.C., Holtfreter, K., Reisig, M.D.: Routine online activity and internet fraud targeting: extending the generality of routine activity theory. *J. Res. Crime Delinq.* **47**(3), 267–296 (2010)
- Poh, G.S., Chin, J.J., Yau, W.C., Choo, K.-K.R., Mohamad, M.S.: Searchable symmetric encryption: designs and challenges. *ACM Comput. Surv.* **50**(3), 1–37 (2017). Article 40
- PWC: US Cybercrime: Rising Risks, Reduced Readiness. Key Findings from the 2014 US State of Cybercrime Survey (2014). <http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf>. Accessed 29 Aug 2017

- Quick, D., Martini, B., Choo, K.-K.R.: *Cloud Storage Forensics*. Syngress, an Imprint of Elsevier, Amsterdam (2013)
- Rogers, A.: From Peer-to-Peer Networks to cloud Computing: How Technology is Redefining Child Pornography Laws (2012). Available at SSRN 2006664
- Samonas, S.: Insider Fraud and Routine Activity Theory (2013). <http://eprints.lse.ac.uk/50344/>. Accessed 29 Aug 2017
- Sawers, P.: Playstation Network and Xbox Live Ddos Arrest: U.K. Authorities Grab an 18-Year-Old Man. *Venture Beat* (2015)
- Smith, R.G.: Responding to organised crime through intervention in recruitment pathways. *Trends Issues Crime Crim. Justice* **473**, 1–6 (2014)
- Stockman, M.: Insider hacking: applying situational crime prevention to a new white-collar crime. In: RIIT Proceedings of the 3rd Annual Conference on Research in Information Technology, pp. 53–56 (2014)
- Stoneburner, G., Hayden, C., Feringa, A.: *Engineering Principles for Information Technology Security (a Baseline for Achieving Security)*. DTIC Document (2001)
- Takabi, H., Joshi, J.B., Ahn, G.J.: Securecloud: towards a comprehensive security framework for cloud computing environments. In: *IEEE 34th Annual Computer Software and Applications Conference Workshops (COMPSACW)*, pp. 393–398. IEEE (2010)
- TrendLabs: *Small Business is Big Business in Cybercrime* (2015). https://www.trendmicro.de/cloud-content/us/pdfs/internet-safety/tlp_small-business-big-for-cybercrime.pdf. Accessed 29 Aug 2017
- Varadharajan, V., Tupakula, U.: Security as a service model for cloud environment. *IEEE Trans. Netw. Serv. Manag.* **11**(1), 60–75 (2014)
- Verizon: *Verizon 2015 Data Breach Investigations Report*. Verizon Enterprise Solutions (2015). http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf. Accessed 29 Aug 2017
- Vidal, C., Choo, K.-K.R.: The current state of an IaaS provider. In: Ko, R., Choo, K.-K.R. (eds.) *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues*, pp. 401–426. Syngress, Boston (2015)
- Willison, R.: Understanding and addressing criminal opportunity: the application of situational crime prevention to is security. *J. Financ. Crime* **7**(3), 201–210 (2000)
- Willison, R., Backhouse, J.: Opportunities for computer crime: considering systems risk from a criminological perspective. *Eur. J. Inf. Syst.* **15**(4), 403–414 (2006)
- Yar, M.: The novelty of ‘Cybercrime’ an assessment in light of routine activity theory. *Eur. J. Criminol.* **2**(4), 407–427 (2005)