
Article:
Y Connolly, L and Wall, DS orcid.org/0000-0002-6003-1592 (2019) The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers and Security, 87. ISSN 0167-4048

https://doi.org/10.1016/j.cose.2019.101568

The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures

Lena Y. Connolly , David S. Wall

PII: S0167-4048(19)30133-6
DOI: https://doi.org/10.1016/j.cose.2019.101568
Article Number: 101568
Reference: COSE 101568

To appear in: *Computers & Security*

Received date: 20 February 2019
Revised date: 9 July 2019
Accepted date: 10 July 2019

Please cite this article as: Lena Y. Connolly , David S. Wall , The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures, *Computers & Security* (2019), doi: https://doi.org/10.1016/j.cose.2019.101568

The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures

Lena Y. Connolly, David S. Wall

Cybercrime Group, Centre for Criminal Justice Studies, School of Law, University of Leeds, UK

Abstract

Year in and year out the increasing adaptivity of offenders has maintained ransomware's position as a major cybersecurity threat. The cybersecurity industry has responded with a similar degree of adaptiveness, but has focussed more upon technical (science) than 'non-technical' (social science) factors. This article explores empirically how organisations and investigators have reacted to the shift in the ransomware landscape from scareware and locker attacks to the almost exclusive use of crypto-ransomware. We outline how, for various reasons, victims and investigators struggle to respond effectively to this form of threat. By drawing upon in-depth interviews with victims and law enforcement officers involved in twenty-six crypto-ransomware attacks between 2014 and 2018 and using an inductive content analysis method, we develop a data-driven taxonomy of crypto-ransomware countermeasures. The findings of the research indicate that responses to crypto-ransomware are made more complex by the nuanced relationship between the technical (malware which encrypts) and the human (social engineering which still instigates most infections) aspects of an attack. As a consequence, there is no simple technological 'silver bullet' that will wipe out the crypto-ransomware threat. Rather, a multi-layered approach is needed which consists of socio-technical measures, zealous front-line managers and active support from senior management.

Keywords: Crypto-ransomware, malware, social engineering, security countermeasures, management support, organisational settings, cybercrime

1. Introduction

In a world of cloud-driven computing, many businesses and organisations now rely wholly upon their IT and data systems to function effectively, to the point that "IT services are becoming a critical infrastructure, much like roads, electricity, tap water and financial services" (Franke, 2017, p.130). Realising the importance of these IT assets to organisations, since early the 2000's cybercriminals have increasingly explored different cyber-tactics to attack businesses (Wall, 2015). In recent years, offenders have sought to extort money via crypto-ransomware attacks. This form of malware scrambles valuable data with virtually-unbreakable encryption and does not release (decrypt) it until a ransom is paid. This is a significant shift from early variants of ransomware such as scareware and lockers and it has increased the impact of ransomware and the overall seriousness of the threat.

This article empirically explores how organisations and investigators have responded to the shift in the ransomware landscape from scareware and locker attacks to the almost exclusive use of crypto-ransomware. In it, we draw upon empirical research to outline how, for various reasons, victims and investigators struggle to respond to this form of threat effectively. In Section 2 we describe changes in the ransomware landscape and explore the strengths and weaknesses of the literature to identify the key research objectives. Section 3 outlines the methodology to undertake the research and in Section 4, we present and discuss our findings. Section 5 concludes.

2. Background

2.1 The Rise of Crypto-Ransomware

As indicated earlier, the ransomware landscape is changing dramatically. In 2018, Sophos found that half (54%) of the organisations they surveyed had been a victim of ransomware in the previous year with an average two attacks each. The healthcare sector was hit most, followed by energy, professional services, and the retail sector. India had the highest level of infection, followed by Mexico, U.S., and Canada. Three quarters (77%) of organisations were running out-of-date endpoint security at the time of the attack and half (54%) did not have specific anti-ransomware protection in place (Sophos, 2019).

Not surprisingly, when organisations are hit by crypto-ransomware, the costs of recovery are considerable. For example, Sophos found in their 2018 survey that the median cost of an attack was $133,000, with most organisations experiencing losses of between $13,000 and $70,000 – a lot of money for a small enterprise which often omits hidden costs such as loss of reputation. These costs are overshadowed by the larger ransomware worm attacks, such as NotPetya, where international shipping firm Maersk is estimated to have lost up to $300 million dollars (Mathews, 2017). The overall cost of ransomware damages for 2017 was estimated to be $5 billion and it is predicted to reach $11.5 billion in 2019 (Morgan, 2018).

In addition to significant financial losses, the risk of ransomware victimisation has increased by 97% since 2017 (Dobran, 2019) and the trend is continuing. Morgan (2018) estimated that by the end of 2019 ransomware will attack a business every 14 seconds decreasing to 11 seconds in 2021. This is compared to 40 seconds in 2016 as reported by Kaspersky (Ivanov et al., 2016). The picture becomes even more gloomy when new forms of attack enablers are considered such as Ransomware-as-a-Service (RaaS) which opens the ‘gates’ to offenders without technical experience.

As the ransomware threat grows, then so does the list of offenders and the increased sophistication of their victimisation techniques. Ransomware actors (especially the enabling brokers who provide RaaS) increasingly employ advanced delivery techniques, including powerful botnets capable of sending millions of malicious messages per day and also Internet scanners that identify vulnerable Internet Protocol (IP) addresses. Furthermore, the use of anonymised platforms on the Dark Web, spoofed email addresses and cryptocurrencies for payments makes it easier for offenders to conceal their digital footprints (Taylor et al., 2019).

All of these developments in the ransomware landscape make it much harder for law enforcement agencies to investigate ransomware crimes and is not helped by the offender’s use of strong encryption which makes it hard for victims to resist the attackers demands. If victims do not have backups in a secure location and the lost information is mission- or safety-critical, the incentive to pay the ransom is high, which strengthens the ransomware business model. Even supposed decryption services have been found to pay the ransom to release the data rather than spend time decrypting it (Dudley and Kao, 2019).

2.2 Related Work

The subject of ransomware has received much attention from academics, practitioners and government bodies (Broadhead, 2018). The FBI (2018), the National Cyber Security Centre (NCSC) (2018) and Europol (2016) issued documents providing guidelines on how to protect organisations from ransomware. The FBI (2018) warned that prevention is the most effective defence against ransomware, and it is critical to take precautions for protection. Security vendors are responding by offering sophisticated technical solutions against ransomware. Since 2016, due to its prevalence, Cyber Threats Reports by the European Union Agency for

Network and Information Security (ENISA) included ransomware as a separate threat from malware, offering relevant information and statistics (ENISA, 2018).

Our search of the scholarly literature revealed that research on ransomware has particularly mushroomed since 2016. We reviewed over 100 academic papers in ScienceDirect, IEEEXplore, ACM Digital, and Google Scholar databases. Technical analysis of ransomware (Subedi et al., 2018; Zimba et al., 2017) has improved our understanding of how this threat operates, subsequently leading to promising remedies. Ransomware countermeasures research emphasised the importance of security education (Simmonds, 2017), policies (Richardson and North, 2017), and technical controls such as detection (Jung and Won, 2018), securely-configured software and hardware (Saxena and Soni, 2018), anti-virus (AV) software (Pathak and Nanded, 2016), email hygiene (Jakobsson, 2017), and Intrusion Prevention System (Adamov and Carlsson, 2017). Organisations are advised to upgrade old systems (Mansfield-Devine, 2018), execute regular patching (Gagneja, 2017), apply the "least privileges" approach (Parkinson, 2017), segregate the network perimeter (Fimin, 2017), and implement effective backup practices (Gonzalez and Hayajneh, 2017). Additionally, several recovery solutions have been proposed to restore (Baek et al., 2018) or decrypt (Kolodenker et al., 2017) files that were scrambled during the attack.

Although the abundance of research in ransomware demonstrates that academic and practitioner communities are acutely aware of the problem and are keen to find suitable solutions, most of the literature on ransomware focuses entirely on technical solutions, with the exception of just a few (for example, Fimin, 2017; Gagneja, 2017; Richardson and North, 2017). Limitations of solely focusing on technical solutions in the context of cyber incidents has been already acknowledged in the academic literature (Connolly et al., 2017a). As Franke (2017, p.131) put it, "security breaches cannot be prevented by technical means alone". Besides, contemporary research acknowledges the importance of an interdisciplinary approach to combatting cyber threats (Choo, 2014). Moreover, despite recent technical advancements (for example, AV software that contains dedicated ransomware protection algorithms in place, advanced email filters etc.), ransomware attacks continue to hurt organisations around the globe.

Ransomware is not simply a technical problem, but an interdisciplinary one (Sittig and Singh, 2016). Offenders increasingly use social engineering techniques to penetrate organisational networks as the first point of entry. The element of extortion includes many psychological tricks in order to force victims to pay, including count-down clocks, explicit warnings of consequences of losing data, an offer to provide security advice in order to avoid subsequent attacks, or a strict deadline to pay with very little time to think (in some cases only 24 hours is given to victims to make the decision). Professional offenders employ business models to assess the optimal ransom amount. Ransomware incidents represent a complex ecosystem and adversary actors exploit a combination of weaknesses comprising of the 'human factor' element, technical shortcomings, the lack of expertise in the security domain, poor leadership and insufficient funding in organisations. Therefore, the objective of this study is to understand the dynamics of crypto-ransomware attacks and inform solutions that will help organisations respond to these incidents. We approach the issue of ransomware holistically and take a more inclusive stance in understanding and defeating this threat.

To the best of our knowledge, no similar research with such a specific focus on crypto-ransomware has yet been conducted. Crypto- is the focus of this paper as it is currently the most prevalent type of ransomware when compared to lockers and scareware, and it inflicts most damage due to its frequent irreversibility. Moreover, empirical investigations of ransomware attacks are rarely reported. Our own literature searches discovered only one

paper by Shinde et al. (2016), in which the authors based their findings on a small-sample survey and two interviews. By collecting data directly from victims, practitioners and police, we developed a comprehensive set of practical recommendations which are illustrated later.

3. Research Method

We adopted a qualitative research approach using an inductive content analysis method as a suitable methodology to reach this study's goal. Qualitative inquiries aim to gain a deep understanding of a phenomenon under study (Maykut and Morehouse, 1994). We conducted a series of qualitative semi-structured interviews and held a focus group through which we probed and explored in order to generate rich data and obtain a deep understanding of crypto-ransomware from an interdisciplinary perspective. Our sample comprised of individuals who had first-hand experience with crypto-ransomware attacks as victims or investigators, the latter included Police Officers from UK's various cybercrime units (CCU). We also drew upon secondary data in the form of interview follow-up emails and confidential Incident Reports shared by victims. These secondary data sources were found to be useful throughout the data analysis for post-interview clarifications and verifying results. In our data collection quest, we were interested in how organisations became infected and how they subsequently recovered. We focused on their self-reflections prior to and during the attacks and also any practices that helped them mitigate attacks and recover quickly. Finally, we drew out any lessons that victims learned as a result of the attacks and looked at the post-attack organisational changes that they implemented. We used the data to develop an all-inclusive taxonomy of crypto-ransomware countermeasures consisting of a) socio-technical measures b) actions for front-line managers and c) senior management. This taxonomy will be useful as the basis for a guide for practitioners which will enable an effective response to crypto-ransomware attacks.

3.1 Sampling strategy

Twenty-six purposefully selected ransomware incidents were explored in depth. The attacks took place between 2014 and 2018. They comprised of diverse crypto-ransomware examples, including recently-emerged variants such as Cerber, Samas, BitPaymer, WannaCry, Dharma, and HiddenTear and older samples such as CryptoWall, CryptoLocker, TeslaCrypt, and KeyHolder. Seeking to find a balance between targeting humans and machines as an initial victimisation point, we included a variety of attack vectors such as malicious emails, brute-force, and drive-by-downloads. Our sample was comprised of organisations of various sizes, industries, and from both public and private sectors. The impact of the ransomware attacks ranged from mild disruptions with a relatively quick recovery to severe outcomes that affected the operation of the businesses for months.

Details of the attacks and the victim organisations who participated in this research are outlined in Table 1. It indicates the victim's industry, organisation size and sector, and attack vector and target (human or machine). To respect the respondents' confidentiality, aliases are used and ransom amounts concealed as they could otherwise be used to identify some of the informants. Also, the names of the ransomware variants and the time of the incidents were intentionally not linked to organisations' aliases to further preserve the respondents' anonymity. These extra precautions helped us gain trust of the interviewees and collect some very sensitive data.

Table 1. A Profile of Respondents, Organisation Type and Attack details

Organisation alias	Industry; size; sector	Attack vector(s)	Attacker target
LawEnfJ	Law enforcement; small; public	Email	Human
GovSecJN	Government; large; public	Email	Human
GovSecJ	Government; large; public	Multiple attacks: 1.Drive-by-download 2.Email 3.Drive-by-download 4.Drive-by-download	Multiple attacks: 1.Machine 2.Human 3.Machine 4.Machine
EducInstF	Education; large; public	Drive-by-download	Machine
EducInstFB	Education; large; public	Brute-force	Machine
LawEnfM	Law enforcement; small	Multiple attacks: 1.Email 2.Email	Multiple attacks: 1.Human 2.Human
GovSecA	Government; large; public	Brute force	Machine
LawEnfJU	Law enforcement; medium; public	Malicious email	Human
HealthSerJU	Health service; large; public	Multiple attacks: 1.Brute-force 2.Malicious email	Multiple attacks: 1.Machine 2.Human
LawEnfF	Law enforcement; medium; public	Malicious email	Human
ITOrgA	IT; small; private	Brute force	Machine
ConstrSupA	Construction; small; private	Brute force	Machine
EducOrgA	Education; small; public	Brute force	Machine
SecOrgM	IT; small; private	Email	Human
ITOrgJL	IT; small; private	Brute force	Machine
CloudProvJL	IT; small; private	Brute force	Machine
InfOrgJL	Infrastructure; medium; private	Brute force	Machine
ConstrSupJ	Construction; small; private	Brute force	Machine
RelOrgJ	Religion; medium; private	Email	Human
SportClubJ	Sport; large; private	Brute force	Machine
UtilOrgD	Utilities; large; private	Brute force	Machine

3.2 Data collection

The data was collected between January and December 2018 and sample interview questions are illustrated in Appendix 1. The majority of interviews were conducted face-to-face, but a few interviews with overseas respondents were conducted by Skype and one was done via email correspondence. Whilst selecting respondents, we sought professionals who had direct experience of dealing with the ransomware incidents. A total of 22 respondents directly participated in the research (5 in the focus group and 17 in interviews). The interviewees included ten IT/Security Managers and Executive Managers with an average of 17 years of professional experience, as well as six Police Officers with an average of 19 years of experience in the field. Additionally, a Security Researcher from a cyber security company with 15 years of experience was interviewed. Finally, a focus group was conducted with four Detective Constables working in the field and a Civilian Cybercrime Investigator who together had an average of seven years in the field. The average duration of interviews was about one hour and ten minutes, resulting in 386 pages of transcribed text in addition to 119 pages of documentation.

In any qualitative research, resource constraints often dictate when data collection ends, however, a point of sufficient "theoretical saturation" is normally reached after about a dozen

or so observations (Miles and Huberman, 1994, pp. 30-31; Eisenhardt, 1989). In this study, we felt that we reached the point of diminishing returns after about twenty cases and in total we examined twenty-six crypto-ransomware incidents even though the incremental learning had already reached a plateau.

2.3 Data analysis procedure

The data analysis consisted of five phases (Figure 1). Phase 1 (open coding) began with reading through transcribed text to "obtain the sense of the whole in order to learn what is going on, before it can be broken down into smaller meaning units" (Bengtsson, 2016, p.11). Each identified unit was first condensed and then labelled with the code (Appendix 2). The process of open coding refers to a non-hierarchical participant-driven deconstruction of data and resulted in 112 distinctive codes (Appendix 3), including positive (1.1.1.1 – 2.5.5.2) and negative (3.1.1.1 – 4.5.3.1) codes. Positive codes represent experiences that helped organisations respond to attacks, while negative codes refer to factors that initiated the infection, facilitated its further spread, and hindered the recovery. Changes implemented after attacks have been also reflected in positive codes.

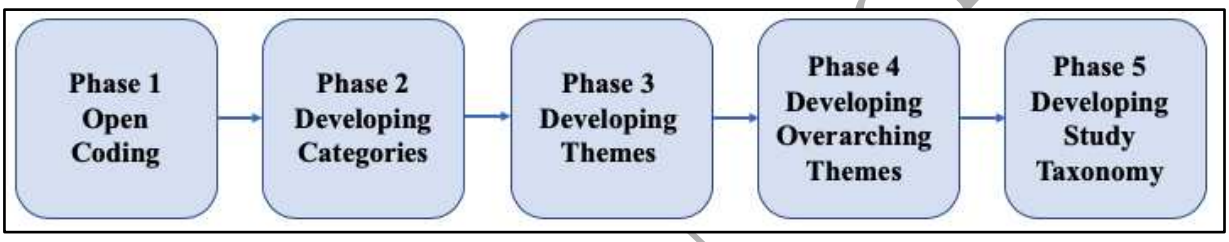

Figure 1. The phases of data analysis.

In Phase 2, the process of categorisation took place (see Figure 2 for greater detail). Categories were identified and units of texts from Phase 1 were sorted into categories. Data units that fitted with the identified categories validated that category. Furthermore, data units that failed to fit with existing categories generated leads to the formation of additional categories. Over the course of this analytical process the categories underwent various changes: while some of them were substantiated quickly, others were eliminated as irrelevant to the focus of inquiry; some were merged due to overlap or needed to be re-defined, and new categories emerged. Due to the large volume of qualitative data, further sorting was required, and categories were grouped into themes in Phase 3 (see Figure 2). Bengtsson (2016, p.12) stressed that "identified themes and categories should be internally homogenous and externally heterogeneous, which means that no data should fall between two groups nor fit into more than one group"; we certainly met this condition. The themes from Phase 3 were further sorted into four overarching themes in Phase 4 (see Figure 2).

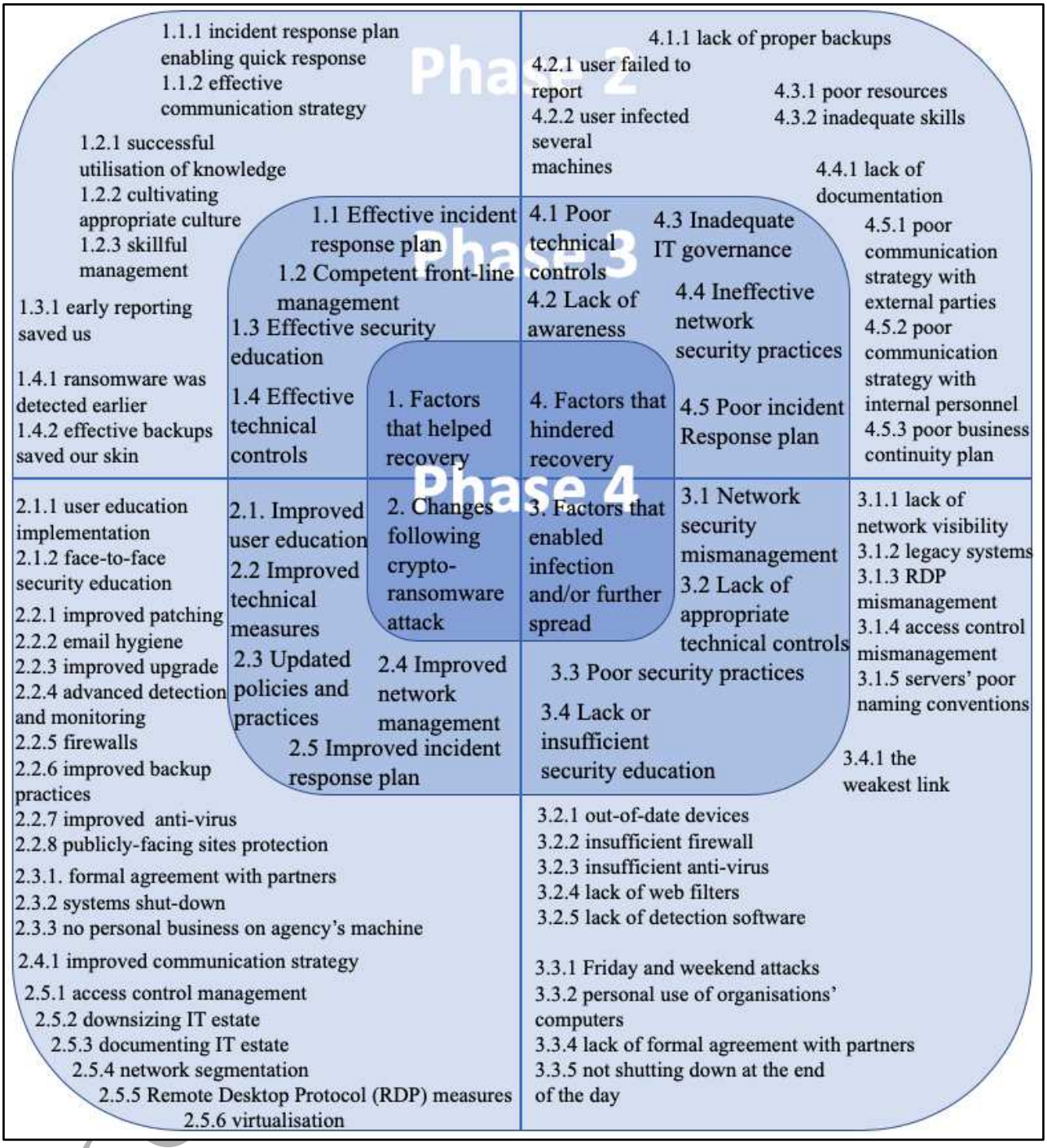

Figure 2. Data analysis results (Expanding phases 2-4).

In the final phase (Phase 5), negative codes were converted into positive, leading to the formation of taxonomy that consists of response tools (controls and measures necessary to implement in organisations in order to respond to crypto-ransomware effectively) and enablers of change (a group of employees who must ensure the organisation is prepared for cyber-attacks) (see Figure 3). To ensure the validity of data analysis, and maintain the quality and trustworthiness of the procedure, each phase was peformed several times. Appendix 2 transparently represents the process from raw data to results required to ensure the quality of analysis. The use of secondary data was a further check on the validity of the data analysis; secondary data was also used througout all phases of data analysis (together with primary data) as an important source of post-interview clarifications.

3.4 Reliability and validity of findings

Several measures were taken to verify the study results and ensure the reliablity of the findings. First, the employment of the purposeful sampling technique prevented sampling distortion. Second, the sample size was determined by the principle of theoretical saturation. Third, secondary data served as an important validator of findings. Fourth, we also asked respondents to provide feedback on interview transcripts and study findings and subsequently made appropriate corrections. Fifth, the results were shared with an experienced researcher from TrendMicro, who provided important expert comments. Sixth, all findings are supported by interviewees' quotes, providing additional verification. Finally, the high degree of unanimity among study informants about the necessary organisational measures to respond to the crypto-ransomware threat suggests that the results are reliable and will not change significantly if additional organisations were to be interviewed. We believe these precautions have eliminated most inaccuracies and misunderstandings from the data collection. . Although we do not claim that the list of proposed measures is exhaustive, the utilisation of the aforementioned measures ensures reasonably reliable results.

As for the validity of findings, the situation is generally more complex if the chosen method is interview because the interview process inevitably allows participants to answer questions in ways that distort the facts. However, in this study, the situation appears to be unique, that is participants had various incentives to provide factual answers. Although we do not claim that the study participants were entirely honest or forthcoming, several factors allow us to conclude that interviewees provided trustworthy replies. First, the majority of victims suffered greatly from crypto-ransomware attacks, including personal emotional distress as well as physical damage to the IT infrastructure. The key incentive for participation in this study was to share their experiences with the aim to prevent future attacks on other organisations. Interviewees appeared to be genuinely concerned with the threat that crypto-ransomware presents, including its recent proliferation and the consequences it may entail, and several respondents strongly disapproved the fact that many organisations are hiding cyber-attacks. Second, several interviewees were appalled by the fact that criminals held them hostages and wanted to 'share their story' and warn other organisations. Third, almost all victims actively participated in validation exercises and expressed a keen interest in receiving final findings. As for Police Officers from the CCUs, the very nature of their job is to reduce cybercrime. Hence, they have a genuine interest in providing objective data. Our observation was that law enforcement representatives readily shared data on ransomware attacks, carefully concealing victims' identities. Other tactics that may have ensured honesty in informants included clearly-communicated anonymity procedures, an option to change or delete parts of text in the transcripts and in this paper, and even to withdraw from the study at any point of time.

4. Study findings and discussion

The taxonomy's components (response tools and enablers of change such as front-line managers and senior management; see Figure 3) were derived from an analysis of the data from semi-structured interviews which sought to obtain respondents' reflections upon their personal experience of responding to crypto-ransomware attacks. These next two sections (4.1 and 4.2) outline the views of the respondents which led to the taxonomy.

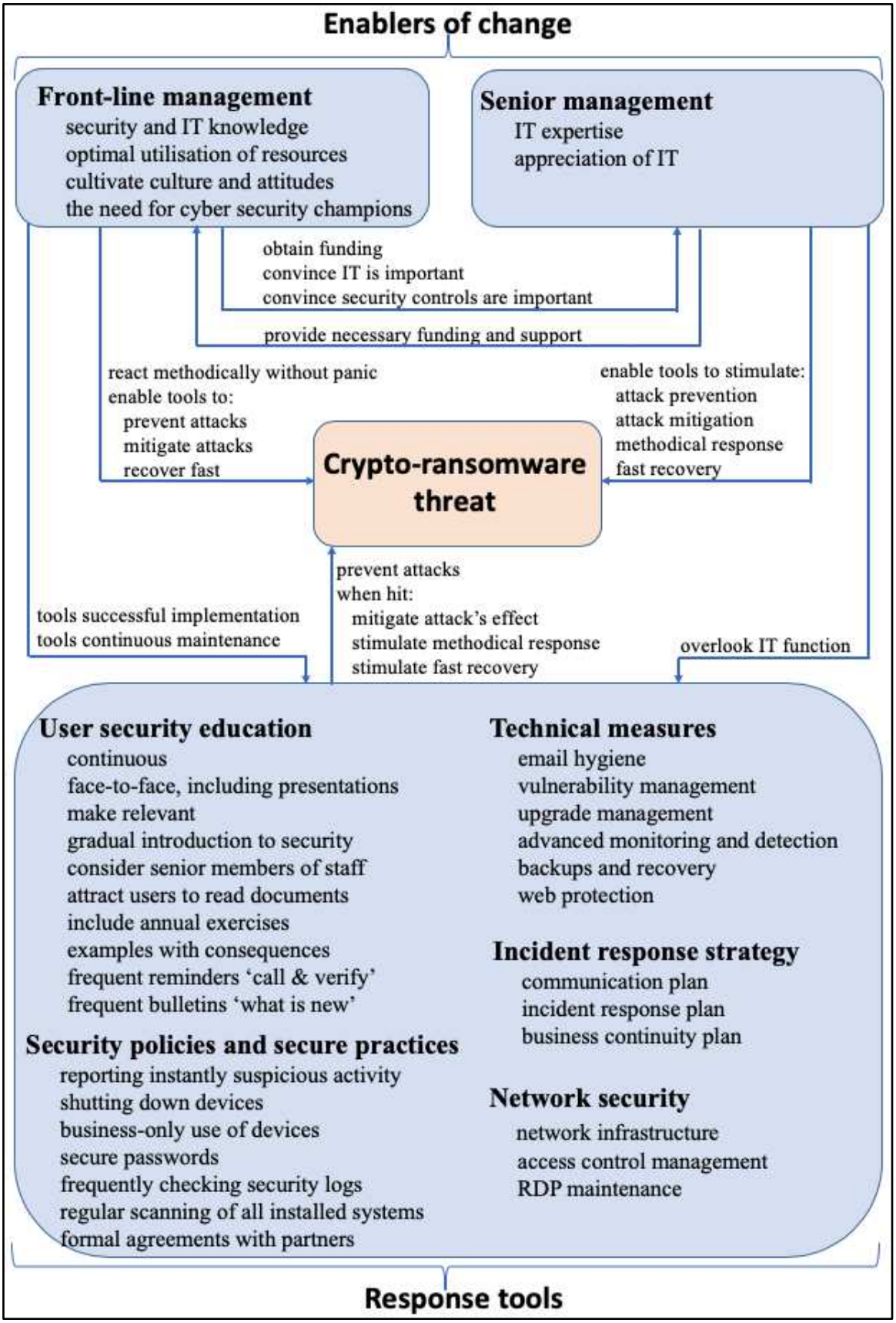

Figure 3. A taxonomy of crypto-ransomware countermeasures

4.1 Response tools

The interviewees felt that an all-round comprehensive approach towards security is absolutely vital in order to protect organisations against ransomware attacks. More specifically, they strongly emphasised the importance of user security education, technical measures, network security, security policies and secure practices, and the incident response strategy as essential response tools to protect organisations against crypto-ransomware (see Figure 3). As the IT/Security Manager, GovSecJN put it:

> "The importance of a comprehensive approach to security cannot be underestimated. That is, not only relying on controls which prevent these sorts of attacks form happening in the first place, but also how you then react when you are hit. Not if you are hit, when you are hit. Because everybody will be hit if you connect to the Internet".

Preparation is therefore essential, but as EducInstFB and GovSecJN warned, even with all the appropriate measures implemented, an organisation can still easily become a victim. Nevertheless, a well-prepared organisation will be able to respond effectively:

> "When the ransomware hit, we were not panicking. We practice good basic security principles, so we were confident. We knew that we had solid backups. We had them in multiple locations and those files that were affected were going to be easy to recover." (IT/Security Manager, LawEnfJ)

GovSecA, in contrast, had no proper security measures in place. Parts of their system were out-of-date, the network management was poor, there was no security education and they lacked an incident response strategy. The organisation also suffered from a chronic lack of funding and poor leadership. Subsequently, the ransomware attack had a severe impact, making it unable to deliver critical services to customers for many months as well as a significant loss of sensitive data. At the time of the interview, GovSecA had already been in a post-attack recovery process for eight months and the interviewee stressed that the recovery was still not completed.

Although our literature search revealed a bias towards technical advancements, our findings suggest that a comprehensive approach to security is essential to counter crypto-ransomware. This is in line with research that focuses on cyber security in general. For example, Kraemer et al. (2009) argued that a comprehensive approach is necessary to strengthen cyber security in organisations. Bulgurcu et al. (2010) stressed that although technical controls help improve security in organisations, relying on them exclusively is seldom enough to combat cyber threats. While organisations invest more in technology-based solutions, the overall number of security incidents is on the rise (Thales, 2018). Indeed, technical controls are important but nevertheless comprise only a portion of the all-inclusive approach developed in this study (Figure 3). The bottom line is that there is no single universal solution to crypto-ransomware attacks. The proverbial silver bullet does not exist; rather, a suite of measures is required which takes on board the taxonomy (Figure 3).

4.1.1 User security education

The interviewees stressed that successful defence starts with user security education, self-defined as continuous, face-to-face, and relevant because "an organisation is as vulnerable as its least savvy user" (Executive Manager, EducInstFB). Education that gradually introduces users to security concepts, takes in consideration senior members of staff, attracts users to read relevant documents, and includes annual exercises, examples to demonstrate consequences, frequent reminders and bulletins/briefings (Figure 3).

In the observed sample, eleven infections out of the twenty-six were initiated by the user. An employee from LawEnfJU, for example, shut down the machine after receiving a ransom note and logged onto several others (one-by-one) hoping to solve the problem, but instead

infected many more nodes on the network. RelOrgJ said that their infection was initiated by a senior individual who had little security education and was not as competent with computers as younger colleagues. An employee from LawEnfM failed to recognise the obvious signs and opened a malicious email; the Executive Police Officer subsequently realised that their online training was ineffective and replaced it with face-to-face education focusing upon social engineering. Following this incident, employees at LawEnfM regularly receive 'call and verify' warnings to contact IT before opening any suspicious content. Several interviewees emphasised the importance of using examples of cyber incidents during training, clearly demonstrating consequences for organisations and employees. IT and security personnel from LawEnfM, LawEnfJ, and GovSecJN issue periodical bulletins as a measure to increase employees' awareness regarding new threats.

The IT/Security Manager from GovSecJ made the important point that security education is a continuous and also a gradual journey; it should begin during an induction process with an initial introduction to security concepts and continue throughout employment to maintain security knowledge. By making education programmes relevant and emphasising that certain threats may have knock-on effects on employees' family members, will have positive influence on their attitudes towards security and lead to security-cautious behaviour at work. Additionally, the IT/Security Manager from GovSecJ recommended annual practical exercises for staff at all levels.

The IT/Security Manager from GovSecJN stressed that one of the most challenging aspects of continuous security education is attracting the user to read security-related documents:

> "You have got to attract people to read the document because they are all very busy. You cannot just say, 'Beware of malware'. Because people get bored and they will not read it. We began sending lots of briefings out which had song names in the title. And it became a thing… so people would look out for it. And go, 'Oh I know what that song is.' Sounds silly, but it worked."

The value of security education is manifold in the academic literature, for example, Connolly et al. (2017b) found that security education increases employee security awareness and as a consequence, security-aware employees are more likely to follow formal controls. Hovav and D'Arcy (2012) and Bulgurcu et al. (2010) found that security education can reduce the level of information systems misuse. Barlow et al. (2013) observed that managing employee security behaviour through a variety of training methods is important. Variety is important because the purpose of security education is to explain to employees how to protect vital organisational assets and why certain rules must be in place (Connolly et al., 2018). The 'why' is particularly vital because if employees do not understand the significance of a certain rule, they may not be able to justify the extra effort they need to make to follow it through and will violate security requirements. Security education must also be repeated if there are any changes in rules and policies in order to ensure that employees keep abreast with organisational requirements (Connolly et al., 2018).

4.1.2 Technical measures

Despite ongoing security awareness and education programmes, GovSecJN and HealthSerJU reported that employees often did not recognise malicious emails sent to their inboxes and subsequently infected the network. In one particular instance, an employee was doubtful about opening an email but in the end decided it was legitimate, only to open a malicious attachment. Several interviewees explained that human error needs to be considered but technical controls are required to support users: "no matter what any organisation does, with all the training in the world, if you send enough emails to an organisation with an exciting looking attachment for someone to click on, someone will click on it" (Detective Sergeant,

CyberBL). Moreover, "if you rely solely on user behaviour, you are going to get infected... It is about having technical controls in place to support the user. And giving staff tools to spot malicious emails" (IT/Security Manager, GovSecJN). A number of technical measures were also suggested by respondents, including email hygiene, backup and recovery procedures, centrally-controlled vulnerability management and upgrades, detection and monitoring, and web protection (Figure 3).

4.1.2.1 Email hygiene

The IT/Security Manager from HealthSerJU reported improvements related to email hygiene, following measures introduced after a user opened a malicious email and infected the network. The measures blocked certain links and attachments and put identifiers in the header of emails coming from external sources. Similarly, LawEnfJ started using a malicious code analysis platform to check suspicious emails. The respondents agreed that although email hygiene will not stop every single malicious email, it will filter out the majority of them. Mohurle and Patil (2017) noted that email is the most common source of ransomware infections, therefore filters must be implemented to avoid malicious emails reaching users' inboxes. Prakash et al. (2017) advised the manual scanning of emails containing links and attachments, even if they seem to come from an authentic user. Referring to Locky attacks, Prakash et al. (2017) stressed that offenders can easily spoof an email address to mislead users as to the source. But modern workplaces demonstrate challenging conditions that involve pressing deadlines, therefore, employees may not have the time to query an email that looks legitimate and will often just click on a link or an attachment. Organisations should therefore assume that every malicious email that makes its way to employee inbox will be opened and plan the implementation of appropriate measures. Hence, relying solely on email hygiene is not effective to protect organisations against crypto-ransomware and additional technological measures are required.

4.1.2.2 Vulnerability management

The respondents also reported that crypto-ransomware managed to take advantage of various software vulnerabilities. Consequently, GovSecA and LawEnfJU implemented a centrally-controlled patching regime of all network devices, including software and hardware updates. LawEnfJU administered mandatory updates within 24 hours of release and recommended – within 30 days. EducInstF made a decision to remove Flash from users' machines. The NCSC (2016) recommends that organisations perform an automated vulnerability assessment of the entire IT estate on a monthly basis. Patches should be applied according to the level of severity of vulnerabilities. Choo (2011), however, stressed that many commercial off-the-shelf products form the backbone of many existing systems, but also contain multiple security vulnerabilities. Jwalapuram (2018) argued that although considerable efforts could be made to develop 'bug-free' software, in practice it is not easily achievable. Subsequently, it is reasonable to expect that organisation cannot possibly patch every single vulnerability and need to invest substantial resources (for example, time and money) into appropriate vulnerability management. Attackers, on the other hand, have to find only one vulnerability to initiate a successful attack.

4.1.2.3 Upgrade management

Upgrade management was highlighted by GovSecA and SportClubJ – these organisations had implemented a system to centrally manage upgrades after ransomware penetrated networks via old machines. The watershed WannaCry attack demonstrated the critical importance of upgrading systems so, upgrades must be assessed and managed centrally and on a regular basis. The NCSC (2016), however, warned about real world limitations that prevent regular

upgrades. In particular, upgrading is costly and may disrupt business operations. Moreover, certain systems may work differently after upgrades, presenting risks to business operations and some specialist applications may not be able to operate on upgraded systems at all. An Executive Manager disclosed that some legacy systems at HealthSerJU cannot be upgraded and therefore require extra protection if ever connected to the Internet. IT specialists advise keeping legacy systems on heavily-protected sub-networks or, if possible, permanently offline.

4.1.2.4 Advanced monitoring and detection

Our respondents indicated that several ransomware incidents occurred due to insufficient or lack of monitoring and detection controls, including AV software and firewalls. Learning from mistakes, HealthSerJU implemented AV systems with an advanced level of protection, LawEnfJ switched to a cloud-based model where security updates are centrally-managed and EducInstF upgraded an AV solution from signature-based to behaviour-based. HealthSerJU and LawEnfJ also installed advanced monitoring and detection software, which proactively feeds information about any new threats and alerts businesses, allowing them to take action before attack campaigns. Moreover, HealthSerJU replaced its old firewalls with advanced versions that provide a higher level of protection and GovSecJN installed software that can recognise and block malicious IPs when ransomware tries to connect back to the control server.

AV software is primarily designed to prevent, detect and remove malware. At best it must offer an advanced level of protection beyond signature-based in order to detect unknown threats. However, not all AV software are the same. Nevertheless, Al-rimy et al. (2018) found that even advanced detection methods have flaws and ransomware may still remain on the network undetected. Sukwong et al. (2011) stressed that users must take precautions before downloading or opening any unknown files. Kaspersky (2018) noted the advantages of cloud-based AV, including automatic updates and a reduced amount of processing power required to keep the system safe, compared to the locally managed AV. Several leading security vendors have developed AV solutions with dedicated ransomware protection in place, though their effectiveness is unknown.

Firewalls are used to filter incoming traffic and can be configured to allow or block packets from specific IP addresses and ports. Sophos (2017) stressed that modern firewalls can effectively defend against ransomware attacks, for example, a sophisticated firewall may include an Intrusion Detection System (IDS) that prevents attacks like WannaCry and NotPetya by performing a deep packet inspection and blocking network exploits such as EternalBlue. The IDS can also recognise connections with malicious IPs and cause routers to terminate them. To support a user at the network entry, a firewall may include a sandboxing technology that identifies suspicious files at the gateway and sends them to a safe location for behavioural analysis. However, Saâdaoui et al. (2014) cautioned that the effectiveness of firewalls mainly depends on the quality of configuration and hence a formal approach to manage firewalls is required. Generally, maintaining firewalls necessitates specialised knowledge. Furthermore, Moore (2010) warned that a firewall is not an ultimate solution to security threats; it is simply one of many tools in a broader cyber security toolkit. Although research on detection is ongoing and assuring; organisations should not solely rely on detection technologies to protect against crypto-ransomware.

4.1.2.5 Backups and recovery

Our respondents stressed that effective backup practices are essential to save organisations from a lengthy recovery and even bankruptcy. These include regular backup procedures,

maintenance of backups in online and offline locations, frequent testing, and processes that ensure a structured recovery, for example, according to the level of criticality of data and applications. EducInstFB, LawEnfM, LawEnfF, ITOrgA, and ITOrgJL all paid the ransom demand because of their ineffective backup procedures and critical data/applications being encrypted. In contrast, LawEnfJ, GovSecJN, GovSecJ, EducInstF, HealthSerJU, CloudProvJL, InfOrgJL, RelOrgJ successfully recovered from crypto-ransomware because they had backups: "What helped us was that we backed up our data up. That ultimately saved our skin." (IT/Security Manager from GovSecJN).

Reflecting on past experiences, the interviewees shared their knowledge relevant to effective backup procedures. For example, the Executive Police Officer from LawEnfM brought attention to faulty backups, where only parts of files were backed up. This was a devastating discovery during the attack, which forced the victim to pay the ransom. Following the incident, the organisation implemented frequent backup testing procedures. Most of GovSecA's backups were retained locally and these became encrypted during the attack. The organisation since moved to a backup solution that includes both online and offline locations. ConstrSupJ admitted firing their external IT provider for failing to maintain effective backups, however, an Executive Manager from EducInstFB warned: "Backups are not like fairy dust… You do not just plug in a backup and suddenly everything is up and running and you are doing well. Recovering from backups is a lengthy process." But, backing up data is a complex process that also requires preparation.

The importance of backups has been stressed in the academic literature (Kumar and Kumar, 2013) as they represent the only real line of technical defence against crypto-ransomware (after the infection takes place). Backups must be recent, regularly tested, and kept in locations inaccessible to ransomware (Al-rimy et al., 2018). Maintaining backups is more challenging in larger networks and adopting a clear recovery strategy is a must.

4.1.2.6 Web protection

Respondents recommended additional measures such as web filters and protection of public-facing websites. Web content filter tools aim to prevent employees from accessing web pages that may potentially contain a malicious content. Although they are effective because they restrict web access, even legitimate sites could become a source of infection as was the case with GovSecJ and EducInstF, where an employee visited a legitimate but infected website and crypto-ransomware penetrated the network via drive-by-download. Besides, web content filtering is not a suitable measure in research-intense organisations, where employees could be prevented from doing their work. Website configuration and vulnerability scanning software can scan web content for vulnerabilities and subsequently increase protection of public-facing websites, however, as with all detection technologies, the problem of newly-emerged vulnerabilities and continuously changing threat landscape remains.

4.1.3 Network security

Unprotected networks allow crypto-ransomware to propagate and infect a large number of nodes. Several victims experienced attacks that led to dramatic consequences due to network security issues, including weak network infrastructure, inappropriate access control management and inefficient maintenance of the RDP (Figure 3).

4.1.3.1 Network infrastructure

Interviewees highlighted several issues which weaken network infrastructures, including poor network visibility, flat network structure, inappropriate naming conventions, unnecessary-large IT estates and inappropriate backup locations. The Executive Manager from EducInstFB, an organisation that is distributed across dozens of buildings, admitted that an

overall lack of network visibility resulted in severe consequences, including hundreds of infected devices, large volumes of sensitive data being encrypted and paralysed critical systems. Prior to the attack, an unlimited number of devices had an unrestricted permission to connect to the network, making these devices invisible. Consequently, the IT department was not able to identify all the locations of crypto-ransomware or assess the extent of the damage. Ultimately, they made the decision to pay criminals and while the majority of data and systems were restored, the recovery process was challenging and lasted for months.

A lack of network visibility is a common problem and Gigamon (2017) warned that two thirds (67%) of organisations have network blind spots, particularly in very large networks, where maintaining visibility is increasingly difficult. Security challenges increase when there is a lack of proper network visibility. More specifically, unaccounted network nodes may contain many vulnerabilities, making an organisation an easy target for cybercriminals. Subsequently, threat detection on so-called 'invisible' machines is impossible. Potentially, an attacker can penetrate network via the 'invisible' machine and stay undetected for prolonged periods of time, assessing network topology and carefully planning subsequent actions. Although maintaining network visibility is essential, it is easier to be achieved in the smaller IT estates. Virtualisation is a potential solution to 'in-house' hardware maintenance, however, cloud computing presents many distributed security risks (Ahmed and Hossain, 2014) which must be prudently assessed. A properly documented IT estate will also increase the overall network visibility, so network segmentation becomes an important security measure as a properly segmented network will make it more difficult for attackers to spread infection (US-CERT, 2016). GovSecA, for example, experienced a substantial attack, in which crypto-ransomware spread to over 100 servers and infected critical systems. The IT/Security Manager acknowledged that the flat network structure allowed the threat to propagate to such an extent. Although network segmentation aims to isolate sensitive data and systems, and can potentially save millions in cyber-attacks (Guta, 2017), the architecture requires specialist knowledge and is costly to implement and maintain.

Other issues related to poor network infrastructure include unnecessarily large IT estates and inappropriate backup locations. After they were attacked, the management at GovSecA realised that numerous vulnerable servers were not even serving a specific purpose within the organisation and removed them. Furthermore, an employee from RelOrgJ was able to work from a backup location demonstrating that the system was not properly set up by IT professionals. As a result of this oversight, the machine got infected and the crypto-ransomware also encrypted backups causing the IT team to restructure the network accordingly in the recovery.

Finally, ITOrgJL experienced a semi-targeted ransomware attack via a vulnerable RDP (as mentioned in section 4.1.3.3). Once inside the network, the attackers manually evaluated its topology, gathering very sensitive information. Due to weak naming convention practices, attackers swiftly identified types of servers on the network. More specifically, the organisation named their servers according to functionality, for example the backup server was named 'backup server', the email server – 'email server', and so on. Although the attack occurred as a result of a combination of factors, this particular weak practice gave attackers the advantage of time.

4.1.3.2 Access control management

Inadequate access control management allows some variants of crypto-ransomware lateral movement across infected networks causing devastating outcomes. Such infections have far greater impact on organisations than attacks on individual systems. An IT/Security Contractor at GovSecA reported that many employees were given administrative rights to

systems they should not have access to, and weak password practices exposed the organisation to a particularly harmful attack, allowing attackers to escalate privileges on the network. During the recovery process, the organisation implemented several measures to strengthen network defences. More specifically, employees' roles and responsibilities were reviewed and documented, and an administrative access was granted appropriately. Two separate accounts were set up for administrators; one under regular user security context for day-to-day work, and another for administrative tasks. Whilst this is a major inconvenience for all users involved, it is a necessary security measure. Furthermore, operation manuals were developed for each business application, clarifying roles, responsibilities, and, subsequently, the level of access for each employee, including senior management.

4.1.3.3 RDP maintenance

ITOrgA, ConstrSupA, EducOrgA, ITOrgJL, CloudProvJL, and ConstrSupJ were infected due to weak RDP practices. Recovery measures therefore included RDP whitelisting, disabling RDP when not in use, employing alternative solutions such as Virtual Private Network (VPN) and appropriate password procedures (for example, using strong and avoiding default passwords, changing passwords frequently). The Detective Sergeant from CyberBL explained that people do not realise that having the RDP turned on is unwise. They tend to use RDP once or twice for a specific purpose then never turn it off:

> "… It is best to switch off RDP. Or even if you were to change the port number to something just random, then it would be much harder to identify. But if you use it on its default port and leave it switched on, you are in trouble … and what we have seen is that approximately 50% of organisations attacked via RDP had password 'password1'. In approximately 25% of the cases, the admin password was the same as the user name. So, if the user was called Bob, the password was Bob."

Although RDP offers some advantages compared to VPNs, the drawbacks must be understood. Some VPN solutions allow to use multi-factor authentication and multiple ports, while RDP does not support that. Moreover, a user can lock down credentials with a certificate of authentication. Therefore, even if an attacker obtained username and password, access to network would be denied without an appropriate security certificate. Not only is the VPN's encryption is stronger compared to RDP, VPNs do not suffer from as many software vulnerabilities as the RDP and connections via VPNs enable a more secure remote access. When set up correctly, VPN allows a remote access without exposing the work computer to the entire Internet. RDP, on the other hand, becomes vulnerable once the connection is established and port 3389 is opened. It is important to note that RDP enables access to the computer, whereas VPN enables access to the network and creates a more secure environment (Scott, 2017).

Keeping networks secure is a challenging task and, as with technical controls, it requires appropriate funding and highly-skilled specialists who can carefully weigh risks against benefits and suggest optimal solutions.

4.1.4 Security policies and secure practices

Many ransomware attacks happened because of weak organisational security policies and practices which made it easier for offenders. An employee from LawEnfJU, for example, was aware that something was wrong, but unsuccessfully tried to fix the problem alone rather than immediately report the suspected malicious activity to IT services. As a result, several additional systems became infected and the opportunity to stop the attack was lost. Following this incident, LawEnfJU implemented a requirement to report suspicious activities immediately.

LawEnfJ, GovSecA, EducInstFB, HealthSerJU and ConstrSupJ were all attacked on a weekend. Such timing gives offenders the opportunity to reconnoitre network topology. Certain variants of ransomware can also stay dormant on the network for an unlimited period, until devices in a 'sleep' mode are turned on by users. A Detective Constable from CyberBR said that:

> "Weekend is a good time for criminals to target any company because everybody leaves work at 4 o'clock on a Friday and do not come back to work until Monday. Especially targeting the server at the weekend is good, because you have not got staff in to try and mitigate any problems."

EducInstFB shared their experience of not shutting down devices:

> "The other vulnerability that created an open door for ransomware is people not shutting down at the end of the day. We all do that. Following the investigation, we did find that this particular ransomware was taking advantage of devices that were asleep. Once ransomware found such devices, it was staying dormant until somebody woke up the device. This poor practice created an open door because we had many dormant devices. If they had been actually truly shut down, the impact of the attack would not be as severe."

The affected organisations subsequently enforced a rule requiring employees to shut computers down at the end of each working day. In addition, reminders to shut down computers were sent to all staff on Fridays and prior to holiday festivities.

LawEnfJ had several partnerships with other organisations, which involved sharing some systems, including email applications. An employee from LawEnfJ received a malicious email into one of the external partner's inbox and opened it on the LawEnfJ's network. An investigation revealed that the partner-organisation did not have appropriate email hygiene. Subsequently, the victim instigated a formal agreement with all external partners on minimal security measures necessary to protect LawEnfJ's network.

A thorough investigation at EducInstF and LawEnfJU revealed that employees used computers for personal reasons, which effectively led to infections. While EducInstF did not implement any changes since the nature of the business would not allow to restrict users' browsing habits, LawEnfJU changed the policy accordingly.

Following a ransomware infection, the IT/Security Manager from LawEnfJU implemented practices such as checking security logs on a daily basis and regularly scanning all installed systems. Furthermore, EducInstFB and GovSecA enforced stricter rules in relation to password practices, obliging employees to create strong passwords, change them frequently, use different passwords at home and work, and keep passwords safe.

Several respondents shared that post-attack changes to security policies were necessary, leading to improved secure practices. A security policy defines rules and guidelines for the proper use of organisational IT resources (D'Arcy et al., 2009). Implementing security policies in organisations is vital for several reasons. First, policies outline rules but also consequences of disobeying these rules. Therefore, policies are viewed as a form of formal sanctions. Prior research demonstrates that sanctions positively influence behaviour in organisational settings (Bulgurcu et al. 2010). Connolly et al. (2018), however, warned that the simple existence of security policies will not have the desired effect. Policies must be visible, up-to-date, easy to follow, properly enforced and tailored to a specific organisational environment or even a department in larger organisations. The most common way of promoting policies is via education and awareness programmes.

Following their ransomware victimisation, LawEnfJ, EducInstFB, LawEnfM, LawEnfJU, ITOrgA and ITOrgJL updated their organisational security policies and practices. The

measures included a mandatory reporting of suspicious activities, shutting down of devices at the end of the day, business-only use of computers, secure passwords, security logs and systems scanning, and formal agreements with partners (Figure 3).

4.1.5 Incident response strategy

Our respondents indicated that the presence of an effective incident response strategy had a direct impact on reducing the consequences of ransomware attacks. The incident response approaches vary in different organisations but typically the strategy represents a suite of documents. Our interviewees specifically brought to our attention the communication plan, the incident response plan and the business continuity plan (Figure 3).

4.1.5.1 Communication plan

GovSecJN and LawEnfJ reported that attention from media and security vendors had a negative impact on the recovery process:

> "Vendors and media, trying to get a hold of us, created 'communication wild west'… They created almost their own denial-of-service because I was trying to do work [recover from ransomware attack] and I was constantly getting phone calls and emails…and people turning up. Dealing with that meant I could not deal with the fallout of the crypto-ransomware attack." (IT/Security Manager, GovSecJN)

Respondents also warned that not only does media attention hamper the recovery process, but it is important to avoid misinformation in media:

> "The media gruesomely exaggerated the ransom amount [from three-digit figure to seven-digit figure]. And within half an hour I had five Police Officers on the doorstep because they thought we were subject to an ongoing live fraud or bribery. And also, vendors…And that was really disappointing actually because we expect security vendors to try and establish fact. And it just did not help because what the effect was – we were overloaded with different parties contacting us…Employees spent a lot of the time worrying about what is going to be said in the press." (IT/Security Manager, GovSecJN)

Following these experiences, the respondents made several changes to their communication plans; for example, the IT/Security Manager from GovSecJN designated a person to deal with external stakeholders during their ongoing cyber-attack. In large organisations, a communication team is usually formed for such purposes. GovSecJN also considered a switchboard to filter calls. Although EducInstF warned about being extremely cautious with wording the messages to the outside world, LawEnfM and EducInstFB suggested that it is important to be transparent with the information on security breaches: "And I can tell you one of the things that really bothers me about all of this – when people keep this behind closed doors, I think that we are giving the advantage to the bad guys" (Executive Manager, EducInstFB).

LawEnfM added that once a security breach becomes public, it is reasonable to expect numerous external parties to contact the victim. However, being reluctant to disclose will only exaggerate the level of hype:

> "My philosophy in general is to let the media know what I can before they come to me. The interest will die down sooner if we share … The media was interested, so we sent out a press release telling them what had happened in general. And, of course, that generated some response. But I think from a tactical perspective we were able to better control the information that goes out." (Executive Police Officer, LawEnfM)

Another important aspect of the communication plan is informing staff throughout the organisation about the attack, including regular employees and management. GovSecJ and GovSecA did not have a clear strategy in place that takes in consideration IT resources being

down, including email. GovSecJ relied on the Internet-dependent telephone line and the communication plan did not include mobile numbers of senior management. Subsequently, the communication channel with executive staff was broken and some big decisions had to be made without consulting top level management. GovSecJ and GovSecJN warned that a robust procedure is necessary to inform all staff across the organisations: "The cascade approach is very useful [top-down method], where you text top level managers first, then they text to middle level managers…and so on until everybody is informed." (IT/Security Manager, GovSecJN)

Prior to the attack, all staff at EducInstFB had emergency application installed on their mobile phones. The application had two channels – one to notify employees and a separate channel to communicate with senior leaders. Such proactive communication method allowed to notify staff immediately. An Executive Manager from EducInstFB also warned about the importance of informing employees about crypto-ransomware attacks due to the nature of this malware. More specifically, the majority of crypto-ransomware variants are able to propagate on networks and certain actions of employees can stimulate the spread (for example, turning on a 'sleeping' device). Besides, the Executive Manager from EducInstFB shared that informed staff can become instrumental to a robust recovery. In this case, they put up posters stating in prominent places "Please Do Not Turn On Or Wake Up Your Computer" because "we were at risk that anybody who came in woke up their computer could have the potential that this thing was lying in wait to lock you down." (Executive Manager, EducInstFB).

4.1.5.2 Incident response plan

LawEnfJ, GovSecJN, HealthSerJU and EducInstFB commented that the incident response plan must include a methodical response to the crypto-ransomware attack, incorporating clearly-documented processes and an accurate description of responsibilities to make vital decisions:

> "An awful lot of lessons were learnt following the attack. We have completely redesigned our major incident response plan as part of this. There is nothing like a live incident to test your processes and most of our processes worked well but a lot of them were undocumented. There is a lot more formalisation of our major incident action plan now. There is a lot more processes and policies which back all of that up." (IT/Security Manager, HealthSerJU)

An IT/Security Manager from GovSecJ also advised to document all decisions made during the attack. Sometimes difficult decisions must be made instantly and later on accounted for. For example, following the attack, GovSecJ disabled the Internet access across the whole organisation in order to prevent infection spread. Essentially, this decision had a negative effect on every user because major communication channels like email and telephony were cut off. Documenting these decisions and the reasons why they were made is vital as senior management will seek an explanation as to why such drastic measures were taken.

Furthermore, the Executive Manager from EducInstFB advised to create a cost account during ongoing incidents:

> "At the time of the crypto-ransomware attack, we had another ongoing major event. We set up separate cost control structures to ensure that any related costs were going into one specific bucket so that when it is time to get the reimbursement, you do not have to do a major reconciliation. When time came to file our claim with our insurer, we just picked up those isolated costs. We did not have to pay a team of accountants to go through thousands of invoices to try and separate them, so that was very important."

4.1.5.3 Business continuity plan

The incident response strategy at GovSecA had numerous scenarios related to different disasters (for example, industrial action, environmental events) but not a cyber-attack with the loss of IT. Such oversight led to the inability to serve customers and hindered a recovery process, for example, one "organisation had business continuity plans in place, but the scenarios were regional emergency scenarios or environmental scenarios. They did not have a scenario in place for a cyber-attack, which greatly deteriorated the recovery process." (IT/Security Contractor, GovSecA). The IT/Security Manager from GovSecJN stressed that business continuity should be coordinated with the incident investigation. An effective investigation of a cyber-attack aims to find the source of the attack and close down all vulnerabilities to prevent further attacks.

Ahmad et al. (2012) stressed that it is inevitable for an organisation that has an Internet connection and uses information and communication technologies to suffer a security breach at some stage. Anderson et al. (2012) noted that although a lot of measures can be taken to prevent and mitigate security incidents, it is not economically feasible to fully protect all systems. Therefore, organisations need to be prepared and react appropriately when cyber-attacks strike (Tøndel et al., 2014). Although an incident response strategy is a complex matter reflected in a suite of documents (for the comprehensive guidelines please refer to standards outlined by ISO/IEC 27035), we specifically focused in this paper on the communication, incident response and business continuity plans (as advised by respondents).

4.2. Enablers of Change

The enablers of change (front-line and senior management) represent a group of employees who must ensure the organisation is prepared for cyber-attacks (Figure 3). The front-line managers (interchangeably referred to as middle or mid-level managers) have a responsibility to implement and maintain appropriate security measures in organisations. In order to achieve this goal, they are required to convince senior management that IT and security are the top priority for the organisation in order to obtain funding. On the other hand, the function of senior management is to ensure that the organisation is ready to respond methodically to cyber-attacks by overlooking IT function and making optimal decisions regarding security funding (Figure 3).

4.2.1 Front-line management

Our respondents suggested that front-line managers must possess certain skills and abilities to be fit for the task (Figure 3). First, management is required to be knowledgeable in the area of security and IT in general. Second, the effective utilisation of external and internal resources is a must skill. Third, front-line management is responsible for harvesting certain cultural traits and attitudes in organisations in order to promote behaviours that compliment organisational security priorities. Finally, organisations need to seek individuals who are not only influential and are able to invoke necessary changes but also hard-working, determined and committed to the job – the true champions (Figure 3).

4.2.1.1 Security and IT knowledge

LawEnfJ, GovSecJN, and GovSecJ demonstrated a methodical and swift response to the crypto-ransomware attack due to front-line managers being security- and IT-savvy. On the contrary, ransomware attacks at GovSecA and EducInstFB took staff by surprise, leading to dire consequences, including a lengthy recovery. The following comments confirm that front-line managers must be knowledgeable in the area of security in order to respond effectively to attacks. The IT/Security Manager from LawEnfJ said that the organisation was well-prepared when the ransomware hit: "I credit that a lot to my knowledge in security side of things…

When I got a phone call informing me that we were under cyber-attack, immediately I had inkling about what it could possibly be. Knowing what to expect definitely helped us recover fast." But the IT/Security Contractor from GovSecA found the opposite in another case:

> "There were two IT staff…they had been here for twenty years…and they left…the organisation only had desk support staff left and they did not understand the architecture of the IT estate… and did not have any documentation to make important decisions. Subsequently, the attack devastated the organisation and the recovery was very lengthy".

4.2.1.2 Optimal utilisation of resources

Victims of ransomware attacks shared their experience on how they utilised various resources during attacks. For example, an Executive Manager from EducInstFB suggested purchasing cyber insurance because their cyber insurer also made several useful recommendations to help with the recovery process and reimbursed the victim some expenses. The IT/Security Manager from LawEnfJU shared that they hired an external cyber response team to help with the incident and they were able to decrypt the scrambled data. The IT/Security Contractor from GovSecA said that their external cyber expert was able to stop the ransomware encryption process and the Executive Manager from EducInstFB recommended engaging a cyber response team and a breach coach before an attack:

> "Find a breach coach [i.e. a lawyer who specifically deals with cyber-breaches and advises clients], find a cyber response team [i.e. to conduct a thorough investigation and find patient zero]…get an engagement set up with them, not a retainer, so there is no need to pay, just an engagement. We wasted time trying to engage with specialists and that was really critical, and I wish we had this engagement."

Several participants suggested caution when choosing an external IT service provider. After being attacked, ConstrSupJ realised that the external IT team failed to maintain proper backups. Subsequently, the victim suffered severe consequences, including the loss of vital information and a lengthy recovery. The Executive Police Officer from LawEnfM had a similar issue with the internal IT team and decided to take the matter in their own hands:

> "When we got hit by ransomware, I was embarrassed, and I was angry... I was angry on two levels. I was upset that we had invited the virus. I was upset at our IT folks because I thought we were protected from this. We had what we thought was an adequate level of security and policies in place for our staff. Unfortunately, the backup software malfunctioned, and our IT folks did not pick up on it. Since the attack, I perform regular cyber threat risk assessments."

The IT/Security Manager from GovSecJN praised the response they received from the external IT provider that happened to be located nearby; the local presence of IT specialists greatly helped the recovery process.

4.2.1.3 Cultivate culture and attitudes

IT/Security Managers from GovSecJN and GovSecJ emphasised the importance of encouraging open reporting culture because a timely response to ransomware is absolutely essential. Without an open reporting culture, staff worry about being subject to disciplinary action. It "discourages people from picking up the phone and telling us about it. We want people to tell us … everybody makes mistakes. So, let's move away from blaming somebody and understand why it happened and what we can do to try and reduce the risk of that happening again." (IT/Security Manager GovSecJN). But the organisational culture also has to harvest a culture of solidarity among its employees. In high-solidarity environments employees understand and share organisational goals; they are cooperative, loyal, and express great satisfaction and pride working for their organisations. On the contrary, in low-solidarity organisations employees believe that organisational problems are not their problems: "An

employee received an email and they should not have clicked on it, but they did. There was a certain amount of apathy. The user said, 'It does not matter, it is not going to affect me.' They were not happy with their working environment." (IT/Security Manager from GovSecJ).

GovSecJN, GovSecJ, EducInstF, EducInstFB, and FinOrgJL added that internal staff solidarity is also the key to an effective recovery. Following attacks, people are forced to work in challenging conditions, including longer hours, the absence of main communication channels and computing devices. Culture of solidarity is an important drive in these challenging circumstances. EducInstFB said that despite a very long recovery process and disabled communication channels, employees stayed supportive and helpful:

> "What was very interesting and hugely important to the recovery process is that we had people without email. We had people who could not Skype. We had people who had no contacts on their phones. And yet everyone was supportive…I still marvel the fact that we had numerous ransom notes and not one was leaked to the press and not one was tweeted out on social media… And it is always good to do great things in the good times, but it is pretty amazing to see people helping in the bad times because that really does say a lot about our culture." (Executive Manager, EducInstFB)

In contrast to the above, GovSecA stressed that while many staff were incredibly positive and went to great lengths to support the recovery (for example, travelling many miles every day for months in order to continue to deliver services), there were employees who complained about difficulties in working during the recovery process and also fed information to the press which fuelled stress among staff and hampered recovery. An Executive Manager from EducInstFB stressed that extra support is needed to encourage employees' cooperation, including open communication, gratitude, and necessary supplies:

> "We believe in open transparent communication and we informed staff immediately…If you tell people what is going on, then they will feel that they are being cared for, and they are far more likely to be supportive. If you leave them in the dark, first, they are going to make stuff up. But second, they are going to feel very agitated because nobody is helping them understand what is going on…Beyond that it is bringing in food, bringing in beverages and doing the walk around and letting employees know that you are there supporting them and recognising them for the great work that they are doing. It was important to let them know that senior management is respectful and appreciative of what they are doing."

GovSecA and GovSecJ suggested that it is also important to change the mindset and attitudes of all staff regarding IT resources. Since the emergence of the digital economy, businesses highly rely on technologies. Cyber-attacks cause prolonged outages, affecting not only IT resources but directly businesses, leading to devastating interruptions in business activities, loss of customers and subsequently soured revenues. In some environments, employees tend to believe that IT staff are at fault of such disruptions. This is, however, a complex problem and the well-being of IT resources depends on several factors. Multiple stakeholders have access to key resources and therefore play an important role in protecting these assets. IT is not a separate entity functioning on its own, but is part of the complex organisational ecosystem. Employees need to understand the importance of IT and take responsibility for keeping these resources safe, while managers at all levels must disseminate this message throughout the organisation. Respondents opined that it often takes a security breach to change attitudes:

> "Following the attack, the cyber threat is on the strategic risk register. So, before everybody knew about malicious software. It was something that happened to somebody else. Post the attack everybody realised the serious impact it can have on an organisation. And attitudes changed all the way through the organisation from the very top to the very bottom. They

understood the danger of malware. And even now when we do presentations to internal teams, people always talk about the malware attack we had. So, it changed attitudes which is good. And it's up to us to make sure that that attitude continues in a positive way." (IT/Security Manager, GovSecJ)

4.2.1.4 The need for cyber security champions

We found that employing cyber security champions who are influential and determined is vital to ensure a proper protection against security incidents. For example, interviewees shared that obtaining funding for cyber security is an extremely challenging task in some organisations. GovSecJ, GovSecJN and GovSecA stressed that one of the main barriers to effective defences against cyber threats, including crypto-ransomware, is the lack of support (often financial) from executive management:

> "Executive managers do not listen to IT managers like me because they are focused on their job… They are not thinking about security and protection. Security is perceived as a second nature or ignored completely. We, front-line managers, need to speak to CEOs and the senior leadership teams or the people that can make those decisions." (IT/Security Manager, GovSecJ)

However, senior management also faces a dilemma over whether they stop providing vital services to the community or spend money on cyber security. IT managers have to get senior management to buy into the concept of security. Moreover, senior managers "do not feel the lack of security is a threat because too many cyber-attacks are still kept quiet out of the fear of incrimination (for example, fines, loss of reputation)." (IT/Security Manager, GovSecJ). Therefore, front-line managers have a challenging task to convince senior management that security controls and IT in general are vital for the organisational well-being.

> "You have got to convince those who have their hands on the purse strings that security presents value to the organisation. Although we have to meet our legal obligations in terms of security but actually, the organisation has lots of legal obligations it has got to meet. And when there is not enough money to go around, some of those legal obligations will fall by the wayside. We compete with other departments. And you have just got to make your business case the best. And we do that by explaining to them the impact of getting it wrong...the consequences of cyber-attacks." (IT/Security Manager, GovSecJN)

Front-line managers are the connecting link between regular employees and senior management. They work closely with staff and directly influence the perceptions and conduct of employees. If middle management perceives cyber security as an important organisational function, this stance inevitably becomes clear to employees and translates into appropriate behaviour. Broadbent and Kitzis (2004) noted that effective managers go beyond pure management and lead by setting expectations and influencing others to change. Van Niekerk and von Solms (2005) found that managers play an important role in fostering cultural traits in organisations. Cheng et al. (2013) concluded that managers should aim to strengthen the relationships between employees and an organisation through a number of actions, including offering employees a sense of achievement and satisfaction; which will, in turn, increase loyalty to the organisational rules. Posey et al. (2011) stressed that managers must demonstrate leadership and knowledge in all aspects of their work in order to influence change. Indeed, all of the above require enthusiastic individuals (true champions) who believe they can inspire required transformations among regular employees and senior management.

4.2.2 Senior management

The efforts of champions, however, may still be in vain. The respondents stressed that it is important for senior management to have IT expertise and to appreciate IT as an organisational function (Figure 3). An IT/Security Contractor shared that at the time of the

attack IT governance at GovSecA was in a poor state. More specifically, the IT Executive did not have technical background and was completely unaware of how to run IT properly. This, in turn, led to many prolonged IT problems and subsequently to an extremely lengthy recovery.

> "Generally, IT gets more and more complicated and it is wrong that the organisations of this size [large organisation] cannot afford a larger IT team. The IT team here is getting squeezed and squeezed. It is not just tiny, it is absolutely tiny. So, you cannot possibly have all of the skills you need for the in-house to manage IT estate" (IT/Security Contractor, GovSecA).

Furthermore, several respondents reported that senior management is often very reluctant to provide funding due to other financial commitments. The IT/Security Manager from GovSecJ warned that the lack of support from senior management will inevitably lead to the poor security posture, making organisations vulnerable to crypto-ransomware attacks:

> "If you do not listen to the protection team, then at one point something is going to break, leaving the organisation vulnerable to attacks … I wrote a report following the ransomware attack, recommending a few actions that we needed to do. We needed to change some processes and implement new processes that were not in place when we needed them. That fell on deaf ears and we were later further attacked…in total, we were attacked four times within 6 months."

HealthSerJU was attacked twice within four months, suffering significantly from both incidents. The IT/Security Manager suggested that both attacks happened because senior management underappreciated the IT function of the organisation and did not provide enough funding for security until the attacks took place: "I think the feeling after both attacks was completely different … Finally, executive management gave IT a profile that it has never had before" (HealthSerJU).

Bailey et al. (2014) stressed that cyber security should be the responsibility of senior management and they must be actively engaged in this process in order to become cyber-resilient. Senior management need to ensure that cyber security measures are implemented across all business functions, driving changes in user behaviour, and endorsing effective governance and reporting in place (Bailey et al., 2014). Furthermore, Hu et al. (2012) reported that senior management participation in information security initiatives had a positive influence on employees' compliance with information security policies. Prior research also demonstrated that a poor security posture of an organisation is directly linked with the senior management's failure to understand their role in the process of implementation security measures (Kolkowska and Dhillon, 2013). Johnson (2017), however, concluded that only 30% of senior business leaders have an in-depth understanding of cyber threats.

5. Conclusion

Crypto-ransomware has become a significant threat over the past several years and the subtle combination of social and technical factors in its ecosystem makes it particularly harmful. In this article we have sought out an interdisciplinary understanding of crypto-ransomware by engaging with individuals who had first-hand experience of either being victims or investigating and learning from their experiences. The findings demonstrate that there is no simple remedy, no silver bullet, for such a complex threat like crypto-ransomware. The attackers are increasingly doing their homework on organisations before they attack and hence are extremely adaptive in both delivering their ever-developing ransomware and tailoring their attack vectors to exploit existing weaknesses within organisations. Successful attacks include psychological trickery, the exploitation of technical shortcomings, neglect by senior management and a shortage of skilled, dedicated and adaptive front-line managers.

Our findings also suggest that organisations generally have to improve their game and be equally adaptive in their responses to attacks. Some of these findings are to be expected, which the research confirms, but more importantly the findings illustrate the nuanced relationship between the technological and social aspects of crypto-ransomware and also their relationship with the organisational setting. As a consequence, our taxonomy of crypto-ransomware countermeasures shows that a multi-layered approach is required to protect organisations and make them more resilient to ransomware attacks, which are increasingly shifting from simple economic crimes of extortion, to disrupting and even destroying organisations and the services they provide.

Our findings, therefore, have important practical implications for IT and security managers and organisations in general. Although generalisation is not typically an attribute of qualitative research, we feel that the findings (like all qualitative studies) provide a deep understanding of crypto-ransomware and we believe that they can be generalised beyond this sample (due to theoretical saturation and purposeful sampling techniques). The taxonomy provides a blueprint for systematising security measures to protect organisations against crypto-ransomware attacks – see 'response tools' in Figure 3. Managers can select controls appropriate to their specific settings, for example, 'business-use only' of IT resources is necessary in some organisations while not practical in others (such as research institutions). Face-to-face security training, for example, may be more possible in smaller organisations than large ones. The taxonomy also underlines the importance of 'social' based controls embedded in organisational cultures, rather than a technical focus to help prevent crypto-ransomware attacks. But our respondents also stated that inappropriate measures, skills and support led to incidents occurring, some of which were particularly devastating. Furthermore, the taxonomy underlines the crucial role that mid-level managers play in responding to crypto-ransomware threats. Our plan is, therefore, to convert the taxonomy into a more user-friendly tool, similar to the Cyber Essentials self-assessment instrument (IASME, 2019). When developing the self-assessment tool, we will initiate discussions with high-calibre cyber security professionals, including security vendors, practitioners and academics.

The skills set for competent front-line management goes beyond being security and IT-savvy. These professionals are required to be influential mid-level leaders who can change attitudes and behaviours in organisations by cultivating certain cultural traits. Therefore, an understanding of the cultural factors and human behaviour is necessary to succeed in this role. They must be true champions and relentless in their attempts to obtain necessary funding from senior management. In return, senior management must be IT-competent and effectively overlook the IT functions of an organisation. Senior managers represent an important part of the security chain in organisations – without an appropriate support all efforts of mid-managers will be in vain. Finally, the findings will assist Police Officers working in CCUs in further understanding the perspective of the victims and also the impacts of crypto-ransomware.

biographical_sketch_connolly

Dr. Lena Y. Connolly

I am a Research Fellow at the Centre for Criminal Justice Studies in the School of Law where I conduct research in the areas of computer security, cryptocurrency and cybercrime. Before joining the University of Leeds, I worked as a Lecturer at the National University of Ireland, Galway with the Business Information Systems group. Website: https://essl.leeds.ac.uk/law/staff/246/dr-lena-y-connolly

biographical_sketch_wall

Prof David S. Wall

I am Professor of Criminology at the Centre for Criminal Justice Studies in the School of Law where I research and teach cybercrime, identity crime, organised crime, policing and intellectual property crime. I have published a wide range of 40+ articles and 12+ books on these subjects and I also have a sustained track record of interdisciplinary funded research in these areas from the EU FP6 & FP7, ESRC, EPSRC, AHRC & other funders, such as the Home Office and DSTL.
Website: https://essl.leeds.ac.uk/law/staff/238/professor-david-s-wall-facss

References

Adamov, A., Carlsson, A. (2017) The state of ransomware. Trends and mitigation techniques, 2017 IEEE East-West Design & Test Symposium, Novi Sad, Serbia, 29 September – 2 October 2017.

Ahmad, A., Hadgkiss, J., Ruighaver, A.B. (2012) Incident response teams – challenges in supporting the organisational security function, Computers & Security, 31 (5), pp. 643-652.

Ahmed, M., Hossain, M.A. (2014) Cloud computing and security issues in the cloud, International Journal of Network Security and Its Applications, 6 (1), pp. 25-36.

Al-rimy, B.A., Maarof, M.A., Shaid, S.Z.M. (2018) Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions, Computers & Security, 74, pp. 144-166.

Anderson, R., Barton, C., Böhme R., Clayton R., Eeten M., Levi M., Moore, T., Savage, R. (2012) Measuring the cost of cybercrime, 11th Workshop on the Economics of Information Security, Berlin, Germany, 25-26 June 2012.

Baek, S., Jung, Y., Mohaisen, A., Lee, S., Nyang, D. (2018) SSD-Insider: Internal defense of solid-state drive against ransomware with perfect data recovery, IEEE 38th International Conference on Distributed Computing Systems, Vienna, Austria, 2-6 July 2018.

Bailey, T., Kaplan, J., Rezek, C. (2014) "Why senior leaders are the front line against cyberattacks", McKinsey Quarterly, June issue, pp. 1-4. [Online]. Available:

https://digitalstrategy.nl/files/2014.06-E-Why-senior-leaders-are-the-front-line-against-cyberattacks1.pdf [Accessed December 2018].

Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R. (2013) Don't make excuses! Discouraging neutralization to reduce IT policy violation, Computers & Security, 39 (Part B), pp. 145-159.

Bengtsson, M. (2016) How to plan and perform qualitative study using content analysis, NursingPlus Open, 2, pp. 8-14.

Broadbent, M., Kitzis, E.S. (2004) The new CIO leader: Setting the agenda and delivering results, Boston, USA: Harvard Business Press.

Broadhead, S. (2018) The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law and Security Review (in press), pp. 1-17.

Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010) Information security policy compliance: an empirical study of rationally-based beliefs and information security awareness, MIS Quarterly, 34 (3), pp. 523-548.

Cheng, L., Ying, L., Wenli, L., Holm, E., Zhai, Q. (2013) Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory, Computers & Security. 39, pp. 447-459.

Choo, K.R. (2011) The cyber threat landscape: Challenges and future research directions, Computers & Security, 30 (8), pp. 719-731.

Choo, K.R. (2014) 'A conceptual interdisciplinary plug-and-play cyber security framework', in H, Kaur & X., Tao (eds.) ICTs and the Millennium Development Goals. Springer: Boston, pp. 81-99.

Connolly, Y.A., Lang, M., Gathegi, J., Tygar, D.J. (2017a) Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study, Information & Computer Security, 25 (2), pp. 118-136.

Connolly, Y.A., Lang, M., Tygar, D.J. (2017b) The impact of procedural security countermeasures on employee security behaviour: A qualitative study, 26th International Conference on Information Systems Development, Larnaca, Cyprus, 6-8 September 2017.

Connolly, L., Lang, M., Tygar, J.D. (2018) 'Employee Security Behaviour: The Importance of Education and Policies in Organisational Settings', in N. Paspallis, M. Raspopulos, C. Barry, M. Lang, H. Linger, C. Schneider (eds.) Advances in Information Systems Development Methods, Tools and Management. Lecture Notes in Information Systems and Organisation. Springer: New York.

D'Arcy, J., Hovav, A., Galletta, D. (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach, Information Systems Research, 20 (1), pp. 1-20.

Dobran, B. (2019) "27 terrifying ransomware statistics and facts you need to read", PhoenixNap, 31 January. [Online] Available: https://phoenixnap.com/blog/ransomware-statistics-facts [Accessed April 2019].

Dudley, R., Kao. J. (2019) The Trade Secret Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers, 15 May, ProPublica. [Online] Available: https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/ [Accessed April 2019].

Eisenhardt, K.M. (1989) Building theories from case study research, Academy of Management Review. 14 (4), pp. 532-550.

European Union Agency for Network and Information Security [ENISA] (2018) "Top 15 Cyber Threats in 2017", ENISA. [Online] Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware [Accessed October 2018].

Europol (2016) "Ransomware: What you need to know", Europol and Check Point, 15 December. [Online] Available from: file:///Users/lena/Downloads/ransomware-what_you_need_to_know%20(1).pdf [Accessed October 2018].

FBI (2018) "How to protect your networks from ransomware", FBI. [Online] Available from: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view [Accessed October 2018].

Fimin, M. (2017) Are employees part of the ransomware problem?, Computer Fraud & Security, 2017 (8), pp. 15-17.

Franke, U. (2017) The cyber insurance market in Sweden, Computers & Security, 68, pp. 130-144.

Gagneja, K.K. (2017) Knowing the ransomware and building defense against it – specific to healthcare institutes, 3rd International Conference on Mobile and Secure Services, Miami Beach, United States, 11-12 February 2017.

Gigamon, M. (2017) "Hide and seek – cybersecurity and cloud", Report, VansonBourne. [Online]. Available: https://www.gigamon.com/content/dam/resource-library/english/analyst-industry-report/Vanson-Bourne-Survey.pdf [Accessed November 2017].

Gonzalez, D., Hayajneh, T. (2017) Detection and prevention of crypto-ransomware, IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, New York, United States, 19-21 October 2017.

Guta, M. (2017) "Network segmentation could save your small business millions in a cyber attack", 21 August, Small Business Trends. [Online]. Available: https://smallbiztrends.com/2017/08/network-segmentation-security.html [Accessed November 2018].

Hovav, A., D'Arcy, J. (2012) Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea, Information & Management. 49 (2), pp. 99-110.

Hu, Q., Dinev, T., Hart, P., Cooke, D. (2012) Managing employee compliance with information security policies: The critical role of senior management and organizational culture, Decision Sciences, 43 (4), pp. 615-659.

Information Assurance Standard [IASME] (2019) Cyber essentials self-assessment preparation booklet, IASME Consortium. [Online] Available: https://www.iasme.co.uk/

[Accessed May 2019].

Ivanov, A., Emm, D., Sinitsyn, F., Pontiroli, S. (2016) Kaspersky security bulletin 2016. The ransomware revolution, 8 December, Secure List. [Online] Available: https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/ [Accessed November 2018].

Kumar S.M., Kumar M.R. (2013) Cryptoviral Extortion: A virus based approach, International Journal of Computer Trends and Technology, 4 (5), pp. 1149-1153.

Kaspersky (2018) "What is cloud antivirus?", Kaspersky. [Online] Available: https://www.kaspersky.co.uk/resource-center/definitions/cloud-antivirus [Accessed November 2018].

Kolkowska, E., Dhillon, G. (2013) "Organizational power and information security rule compliance", Computers & Security. 33, pp. 3-11.

Kolodenker E., Koch W., Stringhini G., Egele M. (2017) PayBreak: Defense Against Cryptographic Ransomware, 12th ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates, 2-6 April 2017.

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

Jakobsson, M. (2017) 'Short paper: Addressing sophisticated email attacks', in: A., Kiayias (eds.) Financial Cryptography and Data Security. Lecture Notes in Computer Science, vol. 10322. Springer: Cham.

Johnson, M. (2017) "Cyber security: the biggest challenges and how to overcome them, Intercity Technology". [Online]. Available: https://intercity.technology/cyber-security-biggest-challenges/ [Accessed November 2018].

Jung, S., Won, Y. (2018) Ransomware detection method based on context-aware entropy analysis, Soft Computing, 22 (20), pp. 6731-6740.

Jwalapuram, P. (2018) "Bug free software, reality or myth?", 29 August, LinkedIn. [Online] Available: https://www.linkedin.com/pulse/bug-free-software-reality-myth-prasad-jwalapuram/ [Accessed April 2019].

Mansfield-Devine (2018) The malware arms race, Computer Fraud and Security, Volume 2018 (2), pp. 15-20.

Mathews. L. (2017) "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million", 16 August, Forbes Magazine. [Online]. Available: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/ [Accessed November 2018].

Maykut, P., Morehouse, R. (1994) Beginning Qualitative Research: A Philosophic and Practical Guide. London: The Falmer Press.

Miles, M. B., Huberman, A. M. (1994) Qualitative Data Analysis: An Expanded Sourcebook, Thousand Oaks, California: Sage.

Mohurle S., Patil M. 2017. A Brief Study of Wannacry Threat: Ransomware Attack 2017, International Journal of Advanced Research in Computer Science, 8(5), pp. 1938-1940.

Moore, G. (2010) "A firewall alone does not provide enough protection", ANX, 19 October. [Online]. Available: http://anxebiz.anx.com/blog/view/a-firewall-alone-does-not-provide-enough-protection [November 2018].

Morgan, S. (2018) "Global ransomware damage costs predicted to reach $20 billion by 2021", Cybersecurity Ventures, 19 October. [Online] Available: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/ [Accessed April 2019].

National Cyber Security Centre [NCSC] (2016) "Vulnerability management", National Cyber Security Centre, 24 September. [Online] Available: https://www.ncsc.gov.uk/guidance/vulnerability-management [Accessed November 2018].

National Cyber Security Centre [NCSC] (2018) "Mitigating malware", National Cyber Security Centre, 9 February. [Online] Available: https://www.ncsc.gov.uk/guidance/mitigating-malware [Accessed October 2018].

Parkinson, S. (2017) Use of access control to minimize ransomware impact, Network Security, 2017 (7), pp. 5-8.

Pathak, P.B., Nanded, Y.M. (2016) A dangerous trend of cybercrime: Ransomware growing challenge, International Journal of Advanced Research in Computer Engineering & Technology, 5 (2), pp. 371-373.

Posey, C., Bennett, R.J., Roberts, T.L. (2011) Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes, Computers & Security. 30 (6-7), pp. 486-497.

Prakash, K.P., Nafis, T., Biswas, S.S. (2017) Preventive measures and incident response for Locky ransomware, International Journal of Advanced Research in Computer Science, 8 (5), pp. 392-395.

Richardson, R., North, M. (2017) Ransomware: Evolution, mitigation and prevention, International Management Review, 13 (1), pp. 10-21.

Saxena, A., Soni, H.K. (2018) Strategies for ransomware removal and prevention, 4th International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, Chennai, India, 27-28 February 2018.

Saådaoui, A, Souayeh, N.B.Y.B., Bouhoula, A. (2014) Formal approach for managing firewall misconfigurations, 8th International Conference on Research Challenges in Information Science, Marrakech, Morocco, 28-30 May 2014.

Scott, J. (2017) "Remotely working: Why VPN is more secure than Remote Desktop Protocol", 10 March, Line Consulting [Online]. Available: https://www.liveconsulting.com/news/remotely-working-why-vpn-is-more-secure-than-remote-desktop-protocol [Accessed December 2018].

Shinde, R., Veeken, P., Schooten, S., Berg, J. (2016) Ransomware: Studying transfer and mitigation, 2016 International Conference on Computing, Analytics and Security Trends, Pune, India, 19-21 December 2016.

Simmonds, M. 2017. How businesses can navigate the growing tide of ransomware attacks, Computer Fraud & Security, 3 (March), pp. 9-12.

Sittig, D. F., Singh, H. (2016) A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks, Applied Clinical Informatics, 7 (2), pp. 624-632.

Sophos (2017) "Best practices to block ransomware with a firewall", 2 October, Sophos. [Online] Available: https://www.techgoondu.com/2017/10/02/best-practices-block-ransomware-firewall/ [Accessed November 2018].

Sophos (2018) "The State of Endpoint Security Today", Sophos. [Online] Available: https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/endpoint-survey-report.pdf [Accessed May 2019].

Subedi, K.P., Budhathoki, D.R., Dasgupta, D. (2018) Forensic analysis of ransomware families using static and dynamic analysis, IEEE Security and Privacy Workshop, San Francisco, United States, 24 May 2018.

Sukwong, O., Kim, H.S., Hoe, J.C. (2011) Commercial antivirus software effectiveness: An empirical study, Computer, 44 (3), pp. 63-70.

Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M., Choo, K. (2019) A systematic literature review of blockchain cyber security, Digital Communications and Networks, 154, pp. 3-13.

Thales (2018) "2018 Thales Data Threat Report – Global Edition", Report. [Online] Available: https://dtr.thalesesecurity.com/pdf/2018-data-threat-report-global-edition-es.pdf [Accessed November 2018].

Tøndel, I.A, Line, M.B., Jaatun, M.G. (2014) Information security incident management: Current practice as reported in the literature, Computers & Security, 45, pp. 42-57.

US-CERT (2016) "The increasing threat to network infrastructure devices and recommended mitigations", Alert (TA16-250A), 6 September. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA16-250A [Accessed November 2018].

Van Niekerk, J., von Solms, R. (2005) A holistic framework for the fostering of an information security sub-culture in organizations, 5th International Information Security for South Africa Conference, Sandton, South Africa, 5-7 July 2005.

Wall, D.S. (2015) Dis-organized Crime: Towards a distributed model of the organization of Cybercrime, The European Review of Organised Crime, 2 (2), pp. 71-90.

Zimba A. (2017) Malware-free intrusion: A novel approach to Ransomware infection vectors. International Journal of Computer Science & Information Security, 15 (2), pp. 317-325.

Appendices

Appendix 1: Sample interview questions

Questions
Can you please describe the experience of the ransomware incident?
How did you find out that the ransomware took hold?
What was the delivery method of ransomware?
Why do you think ransomware was effective in infecting the network?
Does your organisation have specific ransomware policies and training?
Does your organisation have backups?
Were all applications up-to-date prior the attack?
Does your organisation use anti-virus software?
What did you learn from this experience?
What changes have been made in the organisation following the attack?

Appendix 2: An example of an analysis schedule

Meaning unit(s)	Condensed mining unit(s)	Code (Phase 1)	Category (Phase 2)	Theme (Phase 3)	Overarching theme (Phase 4)
In the first instance it starts with users. I have always tried to get companies I work with to teach their employees that human is the weakest link…You are as vulnerable as your least savvy user	In the first instance it starts with users Human is the weakest link You are as vulnerable as your least savvy user	You are as vulnerable as your least savvy user	The weakest link	Lack of or insufficient security education	Factors that enabled infection and/or spread
It is not being ageist or anything, but the individual that initiated infection had not grown up as young individuals with computers, they were in 60s and difficulties with dealing with computers	An individual that infected network was in 60s They had difficulties dealing with computers	Aging employee	The weakest link	Lack of or insufficient security education	Factors that enabled infection and/or spread
The user received a malicious email and they should not have clicked on it. So that was user education. There was a certain amount of apathy. The user said, 'It does not matter, it is not going to affect me.' They were not happy with their working environment.	There was a certain amount of apathy The user was not happy with their working environment	Apathy	The weakest link	Lack of or insufficient security education	Factors that enabled infection and/or spread

Appendix 3: Phase 1 data analysis (open coding)

1.1.1.1 we responded methodically	3.1.3.3 RDP brute-force due to weak password
1.1.1.2 processes were documented in the incident response plan	3.1.3.4 RDP system is not brilliant
1.1.2.1 we handled media invasion very well	3.1.3.5 Microsoft ignored our RDP concerns
1.1.2.2 we were able to inform staff immediately	3.1.3.6 RDP enabled by default
1.2.1.1 breach coach helped enormously with recovery	3.1.3.7 scanning vulnerable IPs on Internet is simple
1.2.1.2 cyber insurance provided information we needed	3.1.3.8 vulnerable Internet facing servers
1.2.1.3 cyber insurance reimbursed many expenses	3.1.4.1 escalated privileges
1.2.1.4 security vendor was helpful	3.1.4.2 poor management of admin passwords
1.2.1.5 cyber experts are needed to find patient zero	3.1.4.3 infected domain controller
1.2.1.6 IT contractors worked very hard	3.1.4.4 disregard for proper network structures
1.2.1.7 IT contractor decrypted scrambled data	3.1.4.5 root access
1.2.1.8 internal staff is the key to successful recovery	3.2.1.1 ransomware came in via vulnerable server
1.2.2.1 timely reporting led to fast reaction to the threat	3.2.1.2 some of our servers were very old
1.2.2.2 it is important to let people know what is happening	3.2.1.3 out-of-date software
1.2.2.3 people were compassionate and determined	3.2.1.4 SMB vulnerability
1.2.2.4 despite of challenging conditions, people were amazing	3.2.1.5 out-of-date Flash
1.2.3.1 security-savvy IT manager	3.2.2.1 low-level protection firewall
1.2.3.2 knowing what to expect helps	3.2.3.1 new malware signature
1.2.3.3 prior experience with attacks helps	3.2.3.2 out-of-date anti-virus
1.3.1.1 early reporting gave us advantage of time	3.2.3.3 drive-by-download
1.4.1.1 we had sophisticate detection software	3.2.4.1 infection came through browsing Internet
1.4.1.2 anti-virus was up-to-date	3.2.5.1 ransomware stayed undetectable for days
1.4.2.1 we frequently test backups	3.3.5.1 signs ‘please do not turn computer on’
1.4.2.2 our offline backups saved us	3.3.5.2 Friday attacks
2.2.1.1 centrally-managed vulnerability management	3.4.1.1 aging employee
2.2.1.2 scheduled vulnerability management	3.4.1.2 apathy
2.2.1.3 removing Flash	3.4.1.3 you are as vulnerable as your least savvy user
2.2.1.4 business applications update	3.4.1.4 convincing email
2.2.2.1 blocking certain attachments and links	3.4.1.5 well-crafted email
2.2.2.2 email identification	3.4.1.6 it starts with user
2.2.2.3 malicious code analysis platform	4.1.1.1 a lot of critical systems did not have backups
2.2.3.1 centrally-controlled upgrades	4.1.1.2 Time Machine was encrypted
2.2.3.2 upgrading legacy systems	4.1.1.3 backups got deleted by ransomware
2.2.3.3 OS upgrade	4.1.1.4 backups were not particularly clever
2.2.4.1 implementation of detection system	4.1.1.5 insufficient backups forced us to pay
2.2.4.2 monitoring software	4.1.1.6 servers were not affected, only desktops and laptops
2.2.5.1 advanced protection firewall	4..1.1.7 backup software was only grabbing chunks of files
2.2.5.2 securely-configured firewall	4.1.1.8 sensitive information was encrypted
2.2.6.1 testing backups	4.1.1.9 too many nodes got encrypted
2.2.6.2 offline backups	4.1.1.10 IT provider failed to ensure efficient backups
2.2.7.1 higher protection anti-virus	4.1.1.11 networked backups
2.4.1.1 considering loss of IT	4.3.1.1 lack of proper funding
2.4.1.2 informing staff via text messages	4.3.1.2 IT team is absolutely tiny
2.5.1.1 applications roles and responsibilities	4.3.1.3 too many servers for such small IT team
2.5.1.2 least privileges approach	4.3.2.1 inappropriate background leading to poor governance
2.5.2.1 retiring old machines	4.3.2.2 senior management incompetence led to further infections
2.5.5.1 disabling RDP	4.3.2.3 not understanding the importance of IT
2.5.5.2 robust VPN to replace RDP	4.3.2.4 senior management should have been more involved
3.1.1.1 we do not know who connects to network	4.3.2.5 underappreciation of IT
3.1.1.2 we do not know amount of ransom notes received	4.5.1.1 phone calls from other organisation caused disruption
3.1.1.3 no control over upgrading/updating OS	4.5.1.2 media invasion
3.1.1.4 it was like a fog when we got infected	4.5.1.3 security vendors invasion
3.1.2.1 legacy systems could not be upgraded	4.5.2.1 we did not realise email will be down
3.1.2.2 legacy systems could not be retired	4.5.2.2 we did not have mobile phones of senior management
3.1.3.1 we do not know who connects via RDP	4.5.2.3 no one thought of IT resources being unavailable
3.1.3.2 we voluntary enabled RDP	4.5.3.1 we did not know how to do both investigation and recovery

Acknowledgements

We would like to extend our sincere gratitude to all respondents for their invaluable contribution to this research. We greatly appreciate interviewees' time and genuine effort. We realise some questions may have brought back emotions experienced by victims during attacks; we would like to thank you for your bravery and willingness to tell your story. We are very grateful for additional inputs during and after data analysis; the comments and corrections provided invaluable contribution in shaping the taxonomy.

Special thanks to Robert McArdle, the Director of Cybercrime Research Team at Trend Micro, who provided priceless comments on technical measures against crypto-ransomware attacks.

We would like to acknowledge the relentless commitment of Police Officers from UK's regional CCUs in providing data and advising on study results.

We would like to thank Dr. Michael Lang for providing instrumental support in improving the paper.

This work was supported by the Engineering and Physical Sciences Research Council and is part of the EMPHASIS (EconoMical, PsycHologicAl and Societal Impact of RanSomware) project [EP/P011721/1].

Please note that the views expressed in this work are ours alone and do not necessarily reflect those of the participants, the commentators or the funding body.