JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2020, 1–18
doi: 10.1093/cybsec/tyaa023
Research paper

Research paper

An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability

Lena Yuryna Connolly [1,*] David S. Wall,[1] Michael Lang [2] and Bruce Oddson[3]

[1]Department of Computer Science, University of Bradford, Bradford, BD7 1DP [2]School of Business and Economics, National University of Ireland Galway, Galway, Ireland and [3]School of Human Kinetics, Laurentian University, Sudbury, ON P3E 2C6, Canada

*Correspondence address. Liberty Building, School of Law, University of Leeds, LS2 9JT, UK. Tel: +44 (0) 113 343 5016; E-mail: alena.yuryna-connolly@fulbrightmail.org

Received 17 October 2019; revised 14 November 2020; accepted 1 December 2020

Abstract

This study looks at the experiences of organizations that have fallen victim to ransomware attacks. Using quantitative and qualitative data of 55 ransomware cases drawn from 50 organizations in the UK and North America, we assessed the severity of the crypto-ransomware attacks experienced and looked at various factors to test if they had an influence on the degree of severity. An organization's size was found to have no effect on the degree of severity of the attack, but the sector was found to be relevant, with private sector organizations feeling the pain much more severely than those in the public sector. Moreover, an organization's security posture influences the degree of severity of a ransomware attack. We did not find that the attack target (i.e. human or machine) or the crypto-ransomware propagation class had any significant bearing on the severity of the outcome, but attacks that were purposefully directed at specific victims wreaked more damage than opportunistic ones.

Key words: ransomware; cybercrime; attack severity; vulnerability factors; victimization; impact assessment

Introduction

In recent years, Europol's annual Internet Organised Crime Threat Assessment report has consistently identified ransomware as a top priority; their latest bulletin states that 'ransomware remains one of the, if not the, most dominant threats, especially for public and private organisations within as well as outside Europe' [1]. Furthermore, as starkly evidenced by an international survey of 5000 IT managers, the incidence of ransomware attacks is growing exponentially [2]. Similar trends have been observed by government and law enforcement bodies [3, 4]. Ransomware attacks can potentially generate substantial financial rewards for offenders, but the ransom – which in most cases is not paid – is just a fraction of the overall cost of the attack in terms of reputational damage and loss of business [3, 5].

Since ransomware first arrived on the scene in a major way about the year 2013, the volume of academic literature produced on this topic has mushroomed. Important advances such as sophisticated detection methods and innovative intrusion prevention systems have been put forward. Organizations are advised to implement effective security education, introduce policies and technical controls, install antivirus software, promote strong e-mail hygiene, upgrade old systems, execute regular patching, apply the 'least privileges' approach, segregate the network perimeter and implement effective backup practices [6, 7]. Although the aforementioned types of work are of tremendous importance to a preventative strategy, they are not by themselves sufficient. This is because most of the research on ransomware to date has focused primarily on its technical aspects, with comparatively little attention being given to understanding the socio-technical side of the attack

or the characteristics of organizations [8]. So, while there is a strong emphasis on developing ransomware countermeasures, there is a lack of studies that examine the real experiences of organizations that have actually fallen victim to ransomware attacks.

It may be tempting to assume certain things about what makes an organization more or less vulnerable to an attack, but we should not be so presumptuous. Although research on cybercrime victimization has significantly expanded over the past two decades, the majority of studies focus on individual-level offences such as online bullying, harassment and stalking. Holt and Bossler [9] make the point that for some types of cybercrime, such as malware and ransomware, our understanding of what causes individuals and organizations to fall victim is not well developed. Our work addresses this limitation by focusing on ransomware crime and collecting data from the actual victims of ransomware.

Generally, the risk of cybercrime victimization has been addressed by studying characteristics of the offender [10], the victim [11] and the crime itself [12]. Our article focuses on the latter two and is motivated by several calls in the literature to better understand typical victims of ransomware attacks, with a view towards developing solutions that prevent or mitigate this sinister problem [9, 13, 14].

To date, only a small number of studies have directly looked at the experiences of organizations that have fallen victim to ransomware. Of these few (see Table 1), the majority consider things at a rather cursory level. Our study, which is based on a substantial sample of 55 ransomware attacks and draws upon qualitative and quantitative data, helps to address this gap in the literature by presenting detailed findings on the antecedents and consequences of actual ransomware attacks within 50 organizations. Our objectives were to

i. Assess the degree of severity of ransomware attacks within organizations;
ii. Explore how characteristics of the organization and characteristics of the attack affect the severity of the outcome.

Review of prior work

Within the literature on cybercrime in general, there have been various efforts to understand the factors that make individuals more prone to becoming victims. Drawing upon Lifestyle Theory and Routine Activity Theory, Agustina [23] proposes several behavioural and environmental factors that should, in theory at least, elevate the risk of being victimized. In practice, however, as found by Ngo and Paternoster [24], these theories do not hold up to empirical scrutiny. Our work differs from these previous studies in two ways: first, we are looking not at cybercrime in general, but specifically at

Table 1. Previous empirical studies of ransomware attacks on organizations

Authors	Country	Method	Sample	Main findings
Choi *et al.* [15]	USA	Quantitative analysis of secondary data	13 reported attacks on police departments from 2013 to 2016	Online lifestyle and cybersecurity stance contribute to ransomware victimization
Zhao *et al.* [16]	USA	Mixed methods case study: questionnaire and interviews	Medical students and surgeons in a hospital that experienced a SamSam ransomware attack (29 survey respondents; 8 interviewees)	Students who are 'digital natives' were seriously stressed by lack of access to electronic resources and were not well adapted to adjust to paper-based workflows
Zhang-Kennedy *et al.* [17]	USA	Mixed methods case study: questionnaire and interviews	Staff and students in a large university that experienced a ransomware attack at a critical time (150 survey respondents; 30 interviewees)	It took several days to recover basic services and the after-effects on user productivity were felt for a considerable time afterward. Substantial data loss and emotional effects on staff.
Hull *et al.* [18]	UK	Mixed methods: questionnaire and interviews	46 questionnaire respondents and 8 interviews (university staff, students and SMEs)	Universities are more likely to be attacked than SMEs; ransomware victims only had basic defences in place
Shinde *et al.* [19]	The Netherlands	Mixed methods: questionnaire and interviews	Snowball sample of 23 individuals and 2 semi-structured interviews	Most ransomware attacks use an untargeted 'shotgun' approach; security awareness among victims was low
Ioanid *et al.* [20]	Romania	Questionnaire	Survey of 123 SMEs	Organization size and turnover is positively correlated with number of attacks; manager education is key prevention factor
Byrne and Thorpe [21]	Ireland	Brief interviews	Three organizations that had suffered attacks	E-mail filtering software had been removed because of the overhead it was placing on IT departments; in the wake of attacks, security training and awareness programmes were ramped up.
Riglietti [22]	Not stated	Content analysis of discussions	301 posts extracted from four online security blogs	Content analysis technique can increase our understanding of security challenges within organizations

ransomware attacks; secondly, our focus is not on individual victims, but rather on organizations.

Although several reports [1–4] suggest that the number of ransomware attacks against businesses continues to rise steadily, it is hard to form any clear sense of the true extent of ransomware attacks. The difficulty of accurately measuring and comparing cybercrime rates has been remarked upon by Furnell *et al.* [25]. Statistics about the incidence of ransomware attacks vary wildly. In an international study based on 574 participants across 77 countries, BCI [26] reported that 31% of respondents had been afflicted by ransomware. In contrast, a large-scale survey of Internet users in Germany revealed that only 3.6% of individuals had suffered a ransomware attack [27]. Simoiu *et al.* [5] estimated that about 2–3% of their sample of 1180 American adults were hit by ransomware between 2016 and 2017. Similarly, Ioanid *et al.* [20] reported that 2% of their sample of 103 Romanian small-to-medium enterprises (SMEs) were affected by the WannaCry attack that year. Against those low incidence rates, Hull *et al.* [18] found that as many as 61% of UK respondents had experienced at least one attack, and Shinde *et al.* [19] reported that 20% of respondents to their survey in the Netherlands were victims of ransomware, although it must be acknowledged that both those studies were based on quite small samples. All of these conflicting survey findings create a rather muddled picture. This, of course, can be put down to differences in sampling methods, response rates, temporal factors and units of analysis, but our essential point is this: it is generally agreed that ransomware presents a grave threat and has adversely affected many organizations, yet we know very little about the experiences of organizations that were attacked or the root causes that left them open to a successful violation.

There are very few empirical studies of the impact of ransomware within organizations or the factors that make organizations vulnerable. Al-Rimy *et al.* [28] present a literature survey of ransomware threat success factors, but the scope of their work extends only to infection vectors and enabling technologies (i.e. cryptography techniques, payment methods, ransomware development kits). They do not consider any organizational or socio-technical factors.

Our extensive search of the literature revealed just a handful of studies that looked directly at the experiences of organizations that were victims of ransomware (see Table 1). To summarize the key findings of these studies: ransomware attacks had major financial and emotional impact on victims, and the common factors that led to the attacks seemed to be a lack of security education or diligence, with organization type and size also emerging as possible factors impacting the likelihood of an attack.

Byrne and Thorpe [21] observe that 'there is a gap in the literature with regards to examining the issue [of ransomware] from a company's perspective and that of its user base.' Our study aims to make a contribution towards addressing this gap. In the next sections, we present a number of factors that we believe might affect the vulnerability of an organization to a ransomware attack, as well as characteristics of the attack weapon and method that could affect the severity of impact.

Hypotheses development

Organization characteristics: size and sector

As with so much of the reported facts and figures pertaining to ransomware, there is disagreement as to whether an organization's size makes it more or less susceptible to attack. An international survey conducted by BCI [26] found that ransomware attacks are a substantially more common problem for large enterprises than they are for SMEs. However, contradictory findings are reported by Beazley [27] who state that SMEs were disproportionately hit by ransomware attacks in 2018, with 71% of all infections occurring within such organizations.

Many SMEs based in the UK believe that they are not likely to be targeted by ransomware attacks; while they place high value on the importance of IT to their business, they are generally not worried about the threat of data loss [29, 30]. SMEs, by their entrepreneurial nature, are more likely to engage in risk-taking behaviour [31]. However, SMEs may underestimate the value to hackers of their information systems and may not realize that they could be targeted as a hop to gain entry into their partners' networks. As Smith [32] puts it, 'even if you think your company has nothing worth stealing, losing access to all your data is no longer an unlikely event.' Kurpjuhn [33] makes the point that SMEs must accept that they are exposed to similar levels of risk as large enterprises but have lower budgets and lesser resources to address those risks.

An argument could be made that larger organizations, simply because they employ more people, are at greater risk of infection due to human error; it only takes one reckless act by a single individual to compromise an entire network. Although not quite the same thing, Bergmann *et al.* [34] found no correlation between the size of a household and the rate of cybercrime victimization experienced by members of that household. How that finding would scale up to larger units in a non-domestic setting is a matter of conjecture, but it seems reasonable to assume that the potential for human error increases relative to the size of the unit.

The purpose of our study is not to determine the relative likelihood of attacks against SMEs or large enterprises. We assume that the probability of attack is much the same, given the indiscriminate nature of ransomware attacks. What we are interested in looking at is the relative impact that attacks have on SMEs as opposed to large enterprises. We therefore explore the following hypothesis:

> *Hypothesis 1a*: An organization's size influences the impact severity of a ransomware attack.

In addition to looking at the effect of organizational size on the impact of the attack, we also want to consider if the sector (i.e. private or public) makes a difference. Prior literature suggests that public organizations, especially universities, hospitals, municipal offices and police departments, are especially prone to attack and have certain characteristics that make them easier targets and more likely to be hit hard [15, 18]. On the contrary, private organizations, especially SMEs or those in customer-facing functions, have much to lose and may not be as capable or as well-resourced as public sector organizations when it comes to withstanding a ransomware attack [35]. In view of the differences between public and private sector organizations, we put forward the following hypothesis:

> *Hypothesis 1b*: An organization's sector influences the impact severity of a ransomware attack.

Security posture

Because ransomware combines technical and social characteristics to create its impact, we explore the organizational victim responses to attacks through the lens of 'security posture'. Security posture is defined as 'the security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation

changes' [36]. Prior research into ransomware attacks on organizations shows that a lack of basic security practices, or failure to comply with them, was a common failing [15, 18]. Organizations that do not have adequate and effective backup strategies are much more likely to end up having to pay the ransom to retrieve their data [15, 28]. Connolly and Wall [8] developed a taxonomy of ransomware countermeasures, emphasizing a multi-layered approach in protecting organizations against ransomware.

While technical defence mechanisms are very important, so too is individual behaviour and good 'online lifestyle'. Inadequate care by employees when choosing to open e-mail attachments or hyperlinks, downloading 'free' versions of software or cracked games, browsing adult content or illegal sports live streams, and installing apps from untrusted sources are all examples of poor online hygiene that can increase the risk of a ransomware infection. Riglietti [28] observed that 'looking at what users say, avoiding infection appears to be a matter of spreading the right security culture within an organisation rather than a technical issue.' A key part of this is education and awareness [37, 38]. In their studies of ransomware victims, Shinde *et al.* [19] and Zhang-Kennedy *et al.* [27] both observed a tendency by employees to assume that cybersecurity was essentially the responsibility of the IT Department. While it is to be expected that the IT Department should take the lead on security and actively promote a strong posture, there is an onus on individuals to utilize good personal security practices and not engage in irresponsible behaviour.

The importance of having good procedures and sticking to them has long been preached, but often not practiced. In the era of ransomware, the penalty for being sloppy or undisciplined when it comes to cybersecurity is potentially very high. For this reason, we wanted to compare the severity of ransomware attacks experienced by organizations with strong security postures to those of organizations that have weaker levels of security. It is with this aim that we propose the following hypothesis:

> *Hypothesis 1c:* An organization's security posture influences the impact severity of a ransomware attack.

Crypto-ransomware propagation class

Since crypto-ransomware was incapable of propagating on networks prior to 2013, we decided to create a simple taxonomy according to the degree of infectiousness (see Table 2). Different propagation classes of crypto-ransomware may have a lesser or greater effect on the outcome of a crypto-ransomware attack as a result of the volume of infection spread.

What we term 'Generation I' crypto-ransomware was not particularly effective in extorting money due to several technological shortcomings, such as the use of easy-to-break encryption, inefficient management of decryption keys and limited propagation capabilities. It is highly likely that Generation I variants are obsolete.

We refer to variants such as CryptoWall, CryptoLocker and CryptoDefence as 'Generation II'. These forms of ransomware initially penetrate networks via desktops or laptops and subsequently take advantage of the local user security context to spread via network paths, encrypting network shares that the user has 'write' access to. They can also encrypt devices physically connected to the infected machine.

What we refer to as 'Generation III.a' malware are those such as Samas and BitPaymer that tend to breach networks via vulnerabilities found in servers [e.g. a weak password in Remote Desktop Protocol (RDP)]. Once inside the server, attackers manually and/or automatically search for various weaknesses within the network (e.g. poor authentication controls, a flat network structure, the lack of network visibility and detection mechanisms). Such vulnerabilities permit attackers to stay undetected and hijack multiple devices and the entire network in some cases. Crypto-worms like WannaCry ('Generation III.b' in our classification) have a similar devastating effect, the chief difference being that they take advantage exclusively of software vulnerabilities in order to propagate.

We are interested in comparing the experiences of victims of Generation II attacks against those of Generation III attacks. The following hypothesis is therefore suggested:

> *Hypothesis 2a:* The crypto-ransomware propagation class influences the impact severity of a ransomware attack.

Attack type and target

As regards the type of crypto-ransomware attacks, the literature distinguishes between 'opportunistic' and 'targeted' incidents [39]. In opportunistic attacks, ransomware is distributed via mass e-mails with the help of powerful botnets that can send millions of messages per day. Offenders do not target any victim in particular but attempt to infect as many machines as possible via a so-called 'spray-and-pray' distribution method. Typically, victims are asked to pay sums between UK£300 and UK£500, an amount that many organizations or individuals can afford to pay, given that the loss of data is unbearable for the victim. Attackers thus attempt to make profit via mass infections. On the contrary, targeted attacks require time and preparation, and offenders typically penetrate networks via spear-phishing or server vulnerabilities. Attackers ask for larger ransoms compared to opportunistic attacks, in the range of 35–100 bitcoins (approximate current value UK£135 000–385 000). Therefore, the consequences of targeted attacks are potentially more severe [40]. Accordingly, we form this hypothesis:

> *Hypothesis 2b*: The attack type, i.e. opportunistic or targeted, influences the impact severity of a ransomware attack.

Another distinction that can be made is between the nature of the target, i.e. 'human' or 'machine'. If the machine is the target, the attack vector will typically be a software vulnerability or weak device passwords, whereas if a human is the target, then the attack vector will be an e-mail message. Cybercriminals can go to considerable rounds to build detailed profiles of their victims before luring them with personalized messages containing malicious attachments or hyperlinks [15, 18]. Since numerous sources allocate a lot of blame to human error and claim that human mistakes cost organizations huge amounts of money [41, 42], it would be interesting to find out if this is the case with crypto-ransomware attacks. We therefore examine the following hypothesis in order to compare attacks aimed at machines against those aimed at humans:

> *Hypothesis 2c*: The attack target, i.e. human or machine, influences the impact severity of a ransomware attack

Research method and analysis of findings

This study used a mixed methods approach following an exploratory sequential design [43]. Phase 1 was qualitative. In order to assess the degree of severity of ransomware attacks (our first objective), we required a measurement instrument. A literature search revealed that there are no readily available tools for this particular purpose. Since crypto-ransomware incidents entail some

Table 2. Classification by crypto-ransomware propagation

Crypto-ransomware propagation class	Description	Examples
Generation I	Early variants of crypto-ransomware were not able to spread on networks and had limited propagation capabilities even within an infected machine (prior 2013).	AIDS Information GPCoder
Generation II	First emerged in 2013, this type can propagate by taking advantage of network paths. Generation II crypto-ransomware can encrypt devices that are physically and logically (e.g. 'write' access to server shares) connected to the infected machine. A common attack vector of Generation II crypto-ransomware is a malicious e-mail.	CryptoLocker CryptoWall CryptoDefence
Generation III.a (Trojans)	First emerged in 2016, this type uses various tools (e.g. password-stealer Mimikatz) and takes advantage of network weaknesses to propagate on infected networks. These variants can infect entire networks, completely crippling an organization's ability to function. Generation III.a crypto-ransomware normally penetrates network via vulnerable servers.	Samas BitPaymer
Generation III.b (Worms)	First emerged in 2017, Generation III.b crypto-ransomware, also commonly referred as 'crypto-worms', takes advantage of software vulnerabilities. Similar to variants like Samas and BitPaymer, crypto-worms can infect entire networks.	WannaCry NotPetya

unique consequences (e.g. encrypted data, disabled systems), we could not use substitutes from other cybercrime studies; the assessment instrument had to be specific to crypto-ransomware attacks. Hence, the aim of Phase 1 was to inductively develop an Impact Assessment Instrument (grounded in empirical data) that can be used to effectively evaluate the severity of crypto-ransomware attacks on organizations in our sample. In Phase 2, we gathered additional quantitative data so as to be able to statistically test our hypotheses.

The Ethics Committee at the University of Leeds approved this research. Consent forms were signed by all study participants. All necessary precautions were followed to ensure the anonymity of study participants and the confidentiality of collected data. The majority of participants were from the UK but there were also a few from North America. Where the names of organizations are subsequently referred to in this article, aliases are used to protect the anonymity of respondents (see Appendix 1). Additionally, interviewees from UK Police Cybercrime Units are given the aliases of CyberRM, CyberLM, CyberTL, CyberBR, CyberBL, CyberTR and CyberCU. Incidents took place between 2014 and 2018.

Phase 1

Sampling strategy and data collection

A purposeful sampling approach was employed to collect data in Phase 1. We conducted 10 semi-structured interviews with professionals from organizations that became victims of ransomware attacks. Interviewees were IT/Security Managers and Executive Managers with an average of 17 years of professional experience. There was one respondent per organization. Since some organizations were attacked more than once, accounts of 15 ransomware incidents were elicited from 10 organizations. Appendix 1 (please refer to first 15 incidents) contains information about the characteristics of attacks and organizations that were interviewed in Phase 1.

In order to enhance the reliability and richness of data, we sought access to individuals who had direct experience of responding to crypto-ransomware incidents. As for crypto-ransomware attacks, the key selection criteria was to include a range of consequences for the victims, varying from low severity (e.g. minimum disruption to business, minimum loss of information, swift recovery) to high impact (e.g. business disruption that lasted for several months, significant loss of critical information, slow recovery).

An interview guide was designed with the aim to learn about participants' perceptions of the attacks' impact and the factors that aggravated or moderated the consequences of these incidents. This exercise guided the development of the Impact Assessment Instrument. Since we planned to use these initial 15 cases in Phase 2 of data analyses, we also ensured to collect profile information about organizations (e.g. size, sector and industry), causes of crypto-ransomware attacks, information about security postures and characteristics of attacks (e.g. attack type, crypto-ransomware propagation class and attack vector). Sample interview questions are provided in Appendix 2. Six interviews were conducted face-to-face, three via Skype with overseas respondents and one via e-mail correspondence.

The decision to stop data collection in qualitative research is made when additional insights are not emerging with new observations. This point is typically achieved after a dozen or so observations [44]. We felt that after examining about 10 ransomware incidents, the incremental learning stopped. But to ensure that the point of 'theoretical saturation' is sufficiently reached, we collected data on 15 cases in total.

Impact Assessment Instrument development (qualitative data analysis)

An inductive content analysis method was used to analyse data and develop the Impact Assessment Instrument. Within the interview transcripts, the impact of crypto-ransomware incidents emerged as a major topic. Interviewees eagerly described their experiences of being attacked, particularly focusing on the consequences of crypto-ransomware attacks. For example, respondents from GovSecJN, EducInstFB, LawEnfM, GovSecA and HealthSerJU spoke in great detail about the despair and distress they experienced. An IT/Security Manager from GovSecJN, a large public sector organization, explained how business continuity disruption affected them:

> There was an impact on service delivery – we could not do what we were supposed to do. It was significant for us. Besides, all our resources were directed towards the incident instead of doing our job.

An IT/Security Manager from LawEnfJU reported a similar experience:

> Ransomware encrypted all of our data files, which, in effect, took the agency offline for about 10 days. This was extremely critical as we could not do our job. We had the server up-and-running in 10

> days and then it took another 10 days to manually re-enter all data. So, the attack critically affected the operations of the department for about 20 days .... The overall impact of this attack was severe, definitely.

An Executive Manager from EducInstFB, a large public organization, shared with us that a Generation III.a crypto-ransomware encrypted hundreds of machines (desktops, laptops and servers). As a result, several critical business functions were disabled and important data were inaccessible. The victim disclosed that various security holes – including ineffective backups, poor patching regimes, the lack of network visibility and feeble access control management practices – led to infection and subsequent dramatic consequences.

GovSecA, a large public organization, suffered an unprecedented attack by Generation III.a crypto-ransomware, where close on 100 servers got encrypted, affecting the operations of the organization for months. Most importantly, the victim lost a lot of critical data because they only had partial backups. At the time of the interview, GovSecA was already in post-attack recovery for 8 months. The interviewee shared that the recovery was still not completed at this point. An IT/Security Manager from GovSecA described their experience as follows:

> We all came back to work on Tuesday morning after a bank holiday weekend and the sun was streaming in through the windows. The cleaners have been in, the office looked great. Everyone felt refreshed after the long weekend. And it took a while for us to realise what happened; that all computing had been turned to stone [encrypted]. Virtually nothing was left untouched. If half of the building had fallen off, you would understand that something has happened. But everything looked great. But it was not – the organisation could not operate.

An Executive Police Officer from LawEnfM, a public SME, described how the organization suffered two ransomware attacks within 2 weeks, affecting critical data:

> We are a full-service law enforcement agency and we have a wide variety of data, some of which is very sensitive. For example, data relevant to criminal incidents like manslaughter cases, child pornography, child sex cases. Several months worth of this data was encrypted, which was pretty significant to us .... While we were recovering after the first attack, we were very unfortunate to get infected by ransomware again.

Comments such as in these few selected excerpts featured regularly in the interviews. We observed that when victims described the impact of ransomware attacks, they focused on factors such as business continuity disruption, recovery time, the number of devices affected, how critical encrypted information was to business and information loss.

On the contrary, interviewees from LawEnfJ and GovSecJ talked about factors that effectively saved the organization from far worse outcomes and emphasized that organizations must be prepared for these attacks or suffer severe consequences. For example, an IT/Security Manager from LawEnfJ, a public SME, shared the following:

> We practice good basic security principles. We have backups in multiple locations .... It comes down to basics like staying up to date with industry. Just recently we went through this massive patching for Intel processors and other processes that could be leveraged into a whole host of attacks .... We were well-prepared for the attack .... We restored everything over a weekend. We were infected on Friday and back up-and-running on Monday.

Similarly, an IT/Security Manager from GovSecJ, a large public organization, explained how they were able to recover with little inconvenience:

> An Incident Management Plan is crucial during cyber-attacks. Instead of running around with our hands up in the area, screaming for help, our response was logical and structured .... We lost some data due to incremental backups but nothing significant that would have stopped an organisation from functioning .... The infection took place at approximately 9 in the morning. By the end of the day, data was restored, and everything was back to normal.

As a result of our data analysis in Phase 1, five categories of negative outcomes emerged from the data, namely 'business continuity disruption timeline', 'recovery time', 'affected devices', 'encrypted information critical to business' and 'information loss'. Under each of these categories, the data enabled us to build impact descriptors ranging across three degrees of severity (low, medium and high). In Table 3, we present the severity descriptors for the five impact categories and corresponding attacks.

Given the broad range of organization types and sectors in our sample, we anticipated that it would be difficult to arrive at a consensus on what constitutes 'Low', 'Medium' and 'High' levels of severity. For example, an outcome that might be regarded as being of 'Low' severity by one respondent could possibly be regarded as 'High' by another, depending on the nature of their business and level of dependency on critical IT systems. However, there was a remarkable degree of consistency among the respondents. There is a general acceptance that any ransomware attack, however minor, is likely to result in an interruption of at least a few days rather than hours. Thus, recovery times and business continuity disruption of a number of days (up to a week) were rated as being on the 'Low' end of the spectrum because, although any disruption is traumatic, in relative terms that is the least amount of time that is expected to be lost. As one interviewee put it,

> Considering the impact and seriousness of the ransomware, it is going to sound strange, but I think that to only lose twelve hours worth of data is an acceptable outcome. If we had not backed up, we would have lost 47,000 files, clearly that would have been a far more significant issue. (IT/Security Manager, GovSecJN)

The Impact Assessment Instrument presented in Table 3 is derived from empirical data and reflects the actual consequences of crypto-ransomware attacks as described by the victims. All five of the items shown in the table are components of the overall severity of a ransomware attack. Because the five items are measured on a three-point ordinal scale, as opposed to a multiple-point continuous scale, we used the ordinal alpha coefficient [45] to test for internal reliability. The value for ordinal $\alpha = 0.96$ which indicates a high degree of agreement between the five items.

To compute a composite score for overall severity, we considered using the average or median of the five items but decided to use the maximum. The logic behind this reasoning is that if any of the items is evaluated as 'High', it means that the attack represented a serious shock to the organization with major consequences. Therefore, a 'High' severity value for any single item trumps all the others, even if they all have lesser values. This also gets around the aforementioned problem whereby the assessment instrument might misevaluate a particular item as 'Low' when in fact, because of the organization's circumstances, it should be 'High'; in such cases, the likelihood is that at least one other item would have a 'High' rating and hence the overall severity would correctly be evaluated as 'High'.

Table 3. Impact Assessment Instrument and corresponding victims

Impact item	Degree of severity (3-point ordinal scale)		
	1 = Low	2 = Medium	3 = High
Business continuity disruption timeframe	Up to 1 week	Up to 2 weeks	More than 2 weeks
Recovery time	Up to 1 week	Up to 1 month	Several months or more, if at all
Affected devices	One or more user devices, possibly including shares on one or more servers	Several devices and more than one server; or where a central server is encrypted affecting not just individual users but the functioning of a whole department	All or majority of devices, completely or almost completely crippling IT systems
Encrypted information critical to business	Some data compromised, but nothing critical	Data critical to some business functions of low to medium priority	Data critical to majority of business functions, or some high priority function(s)
Information loss	No loss, or some loss acceptable with incremental backups	Loss affecting some critical business functions	Loss affecting all or majority of critical business functions

Next, using the Impact Assessment Instrument shown in Table 3, we analysed all of the initial 15 cases (interview transcripts) to determine the extent of the attack impact. We assigned the degree of severity for all five categories for each impact item. An exemplar of this assessment exercise is provided in Appendix 3.

We were conscious of the limitation that the initial version of the Impact Assessment Instrument was based on data collected from 10 public organizations, with no private businesses. To remedy this, as we collected data on a further 45 cases, including both public and private organizations, we asked interviewees to assess the severity of ransomware attacks using our scale (i.e. low, medium, high) and comment on the reasons for their answer. The purpose of this exercise was to validate our instrument and confirm that the categories that emerged initially were relevant across the whole sample. We also validated the instrument by consulting with experienced police officers. We found that the instrument gave a reliable measure of the severity of an incident as perceived by the victim.

Phase 2

Sampling strategy and data collection

In order to test our hypotheses, we required to collect more data on crypto-ransomware incidents. It has been widely acknowledged that collecting data on cyberattacks is extremely difficult. In Phase 1, it took us over 6 months to find organizations that were willing to share sensitive matters relevant to the attacks. Therefore, we made a decision to approach the data collection matter differently in Phase 2. Instead, we sought out police officers from UK Cybercrime Units who had extensive experience in dealing with crypto-ransomware attacks. Mainly, such experience included helping organizations to effectively respond to the attacks, understanding what caused them, providing emotional support to victims if necessary and offering post-attack advice. Our expectation was that each police officer would be able to provide relevant information on several ransomware incidents at the time, which would make the process of data collection more manageable.

We succeeded to connect with 10 police officers (four Detective Sergeants and six Detective Constables) and 1 Civilian Cybercrime Investigator, who provided information on 22 usable ransomware incidents via semi-structured interviews and one focus group. Two police officers were interviewed twice as they were able to add new information. The average professional experience of the study respondents was 19 years. We also managed to collect data on 22 more cases with a Detective Inspector, who, unfortunately, was not able to meet with us face-to-face but agreed to provide data via a structured questionnaire (sent over e-mail). Additionally, we interviewed an IT/Security Manager with over 20 years of professional experience, which added one final case to our database of ransomware incidents. Relevant information is available in Appendix 1 (Cases 16–60). Due to the aforementioned access constraints, a snowballing technique was used to collect data for Phase 2.

The questionnaire and second phase interview guide (see Appendix 4) were based on the Impact Assessment Instrument and hypotheses. We asked questions that would help us to assess the impact of an attack. We also collected profile information on organizations (e.g. size, sector and industry) and characteristics of attacks (e.g. attack type, crypto-ransomware propagation class and attack target). Additionally, we included questions that would help us classify the security posture of each organization. For this purpose, we used the taxonomy of crypto-ransomware countermeasures developed in our previous work [8]. The headings from this taxonomy served as a guide for questions. Therefore, in order to assess a security posture of organization victims, we asked interviewees about security education, policies and practices, technical measures and network security, the incident response strategy and the attitudes of management towards cybersecurity (see Appendix 5).

Overall, 45 additional cases of ransomware attacks were examined in Phase 2, bringing the total to 60 cases. For five of the 60 cases, there was insufficient data to be able to determine the overall impact severity, so those cases were discarded as being unusable, leaving us with 55 usable cases. Although a snowballing technique was used to collect data in Phase 2, our overall sample included organizations of different sizes and from different sectors. Attacks were recorded against both humans and machines by different crypto-ransomware propagation classes. Different levels of security posture were noted among participants, ranging from weak to strong. Finally, the sample contained opportunistic attacks as well as targeted ones.

For a few of the cases, we did not have values for all of the five items in the Impact Assessment; in those cases, we evaluated the overall impact based on the maximum of the items for which we had values, supported by an inspection of qualitative data from those cases. We found that this method of computing the composite score for overall severity gave the most accurate results, as validated using participants' personal assessment of the attack impact and our own judgement based on what we gleaned from interviews. Results of the assessment exercise are available in Table 4.

Table 4. Impact Assessment Instrument and observed frequencies among respondents ($n = 55$)

Impact item	Degree of severity (3-point ordinal scale)		
	1 = Low	2 = Medium	3 = High
Business continuity disruption timeframe ($n = 52$)	Up to 1 week (65%)	Up to 2 weeks (14%)	More than 2 weeks (21%)
Recovery time ($n = 51$)	Up to 1 week (59%)	Up to 1 month (22%)	Several months or more, if at all (19%)
Affected devices ($n = 53$)	One or more user devices, possibly including shares on one or more servers (53%)	Several devices and more than one server; or where a central server is encrypted affecting not just individual users but the functioning of a whole department (19%)	All or majority of devices, completely or almost completely crippling IT systems (28%)
Encrypted information critical to business ($n = 51$)	Some data compromised, but nothing critical (29%)	Data critical to some business functions of low to medium priority (24%)	Data critical to majority of business functions, or some high priority function(s) (47%)
Information loss ($n = 47$)	No loss or some loss acceptable with incremental backups (57%)	Loss affecting some critical business functions (32%)	Loss affecting all or majority of critical business functions (11%)
Overall impact severity (composite score) ($n = 55$)	Low (27%)	Medium (20%)	High (53%)

Note: Overall $n = 55$ but item response rates ranged from 85% (47) to 96% (53).

Quantitative data analysis

Overall, our sample included 50 organizations of different sizes, sectors (i.e. public or private) and industries (55 usable cases of crypto-ransomware attacks). Totally, 35 (70%) of the organizations were SMEs, while 15 (30%) were large organizations. We used the European Commission guidance to define the organization's size [46]. The industries were broad and varied, including IT, government, law enforcement, education, healthcare, financial services, construction, retail, logistics, utility providers and several other categories. Of the 50 organizations, 19 (38%) were in the public sector and 31 (62%) were in the private sector. Five (10%) were located in the North America and 45 (90%) in the UK (see Appendix 7). Security postures were determined for 34 of the 50 organizations (see Table 5). Twenty organizations (59%) had a weak security posture, 13 (38%) had a medium-security posture and only one had a strong posture. We used the criteria outlined in Appendices 5 and 6 to assess the security postures of organizations.

Except where otherwise stated, the hypotheses were assessed using two-sided Fisher's Exact tests. The size of our sample provides acceptable power to detect moderate-to-large relationships between categorical variables using this technique. Where data was missing, cases were excluded; the number of relevant cases (n) is stated in the results of each test.

We found that the degree of severity of a ransomware attack did not vary by organizational size, $P = 0.542$. Indeed, the majority of attacks in both SMEs and large organizations were of high severity (57% and 53%, respectively).

The severity did, however, vary according to organizational sector. Private organizations were considerably more likely than public organizations to experience serious negative consequences as a result of ransomware attacks, $P = 0.044$. Of the private organizations, 68% were hit by attacks of the highest severity, whereas a much lower percentage (37%) of public organizations were as badly affected. This finding supports Hypothesis 1b.

Most tellingly, impacts also varied with organizational security posture, such that those organizations with weak security postures were far more likely to experience a severe impact than were those with medium or strong postures, $n = 34$, $P < 0.001$. Of the organizations that had a weak posture, 80% had been hit by ransomware attacks of high severity. Thus, Hypothesis 1c is also supported.

Post hoc, we found that security posture did not differ according to organization size, with the majority of organizations – 57% of SMEs and 64% of large organizations – having a weak security posture. However, when looking at the relationship between organization sector and security posture, a significant difference ($P = 0.035$) was observed. Public organizations had considerably stronger security postures than those in the private sector. This may partly explain why the impact of attacks on public sector organizations was not as severe.

As can be seen in Appendix 1, the 50 organizations spanned 23 different industries (i.e. financial services, healthcare, retail, etc.) so it was not meaningful to conduct correlation analysis on this variable as the numbers were spread too thin. However, one observation that stands out is that of the seven respondents from the IT industry, six of them (86%) experienced attacks of high severity. This is above average and somewhat surprising, although with such a small subsample it is not possible to draw reliable inferences.

Looking then at the crypto-ransomware propagation classes, 32 (58%) were of type Generation II, while 23 (42%) were of type Generation III (Generation III.a and Generation III.b classes were merged in data analysis due to similar propagation characteristics). Totally, 38 attacks (72%) were opportunistic and 15 (28%) were targeted. Twenty-five attacks (47%) were targeted at humans and 28 (53%) aimed at machines (see Table 6).

The degree of severity did not vary with the crypto-ransomware propagation class (i.e. Generation II vs. Generation III) $n = 55$, $P = 0.334$, nor with the attack target (i.e. human vs. machine), $n = 53$, $P = 0.813$.

The type of the attack (opportunistic vs. targeted) was also considered. Targeted attacks were more likely than opportunistic ones to lead to severe consequences, $n = 53$, $P = 0.063$. 80% of targeted attacks gave rise to impacts of high severity, whereas a considerably lower proportion of opportunistic attacks (45%) had high negative consequences. This difference is statistically significant (Mann–Whitney $U = 177$, $P = 0.02$) so we are inclined to accept Hypothesis 2b.

Post hoc, companies with a weak posture were much more likely to be targeted via machine vulnerabilities as a point of entry, whereas companies with medium or strong security postures were more likely to be attacked via social engineering tricks ($n = 34$, $P =$

Table 5. Cross-tabulations for Hypotheses 1a, 1 b and 1c

	Attack severity, *n* (%)		
	Low	Medium	High
H1a: Organization size ($n = 50$)			
SME	7 (20)	8 (23)	20 (57)
Large	5 (33)	2 (13)	8 (53)
H1b: Sector ($n = 50$)*			
Public	5 (26)	7 (37)	7 (37)
Private	7 (23)	3 (10)	21 (68)
H1c: Security posture ($n = 34$)***			
Weak	0 (0)	4 (20)	16 (80)
Medium	4 (31)	6 (46)	3 (23)
Strong	1 (100)	0 (0)	0 (0)

*$P < 0.05$; ***$P < 0.001$.

Table 6. Cross-tabulations for Hypotheses 2a, 2 b and 2c

	Attack severity, *n* (%)		
	Low	Medium	High
H2a: Crypto-ransomware type ($n = 55$)			
Generation II	10 (31)	8 (25)	14 (44)
Generation III	5 (22)	3 (13)	15 (65)
H2b: Attack target ($n = 53$)			
Human	5 (20)	6 (24)	14 (56)
Machine	8 (29)	5 (18)	15 (54)
H2c: Attack type ($n = 53$)*			
Opportunistic	12 (32)	9 (24)	17 (45)
Targeted	1 (7)	2 (13)	12 (80)

*$P < 0.1$.

0.019). We also observed that 91% of targeted attacks were against organizations that had weak security posture. Table 7 demonstrates results of hypotheses tests.

Interpretation and discussion

Organization size does not matter, ransomware is indiscriminate

Within the observed sample, organization size, by itself, did not affect the severity of attacks. As outlined in 'Organisation characteristics: size and sector' section, prior findings and opinions on the relationship between organization size and the incidence of ransomware attacks are rather inconsistent, with some saying that ransomware is mainly a problem for large enterprises and others saying that SMEs make up the bulk of the victims. Of the organizations that we observed, SMEs and large organizations were similarly impacted by ransomware attacks and in most cases the impact felt was of high severity. This result is consistent with interpretations expressed by police officers from UK Cybercrime Units:

> Ransomware is indiscriminate. It does not choose its victims. It chooses computers and those computers can be owned by anybody. (Detective Sergeant, CyberBL)
>
> Ransomware does not target organisations of a particular size. All organisations, small, medium and large, are equally affected. (Detective Sergeant, CyberRM)

Table 7. Results of hypothesis tests

Hypothesis	Result
Hypothesis 1a: An organization's size influences the degree of severity of a ransomware attack	Rejected
Hypothesis 1b: An organization's sector influences the degree of severity of a ransomware attack	Accepted
Hypothesis 1c: An organization's security posture influences the degree of severity of a ransomware attack	Accepted
Hypothesis 2a: The crypto-ransomware propagation class influences the impact severity of a ransomware attack	Rejected
Hypothesis 2b: The attack type, i.e. opportunistic or targeted, influences the degree of severity of a ransomware attack	Accepted
Hypothesis 2c: The attack target, i.e. human or machine, influences the degree of severity of a ransomware attack	Rejected

We observed several large organizations that experienced severe consequences of crypto-ransomware attacks (e.g. EducInstFB, GovSecA, HealthSerJU, SportClubJ, etc.) as well as SMEs (e.g. LawEnfJU, LawEnfF, ITOrgA, ConstrSupA, etc.). Therefore, regardless of how large or small an organization is, there is no room for complacency. SMEs often baulk at spending their limited funds on IT security measures, weighing things up on the basis of the financial cost of countermeasures vs. the expected probability and expected impact of an attack [30]. While we cannot offer any insights into the probability of an attack, we can speak about impact. Our findings show that if an organization has weak defence mechanisms, then regardless of whether it is an indigenous start-up or a large multi-national corporation, it is likely to experience very severe consequences in the event of a ransomware attack, such as having critical systems knocked out, heavy data losses and major disruptions of several weeks or more.

Private sector organizations are more likely to experience severe effects

Private sector organizations were more likely to report severe impacts than were those in the public sector in the sample observed in this study. This finding can be explained by the very nature of public organizations as compared to private businesses. Public sector organizations are generally state-owned with an obligation to provide some universal service such as healthcare, education, policing, or civic administration. The private sector, on the contrary, is mainly composed of organizations whose ultimate purpose is not to serve the public but to generate profit. Cyberattacks on profit-driven organizations normally lead to substantial financial losses, reputational damage and loss of customers; the series of security breaches on TalkTalk is one such example [47]. If public organizations such as councils, state agencies and police departments experience a cyberattack, they may lose public confidence, but as sole suppliers they are not going to lose customers or revenue as they are publicly funded. As an IT/Security Manager from GovSecJN (a public organization fully funded by the UK government) explained:

> Yes, there was a financial impact because resources were directed towards dealing with the cyber-attack. But it is difficult for us to quantify the financial impact .... The impact is different for us. It is the impact on service delivery to public. How we care for

children. How we care for adults. Even road potholes – people could not report potholes because our systems were down.

Information from interviews with police officers working in the UK Cybercrime Units confirmed our impression that private sector organizations suffer more severe consequences; e.g. a specialist detective within the CyberTL unit told us based on his extensive experience that:

> Cybercriminals know that the private sector depends on customer service. They know that these organisations will pay. Especially, we find that a lot of IT companies have been hit. I do not think this is because IT companies are more prone to targeting. It is just because when they are hit by ransomware, it is so much more devastating for them due to their dependency on customers.

This observation is in line with our finding that 86% of respondents from the IT industry experienced attacks of high severity. However, it should be noted that our sample is based on attack victims only and is not representative of the number of potential organizations in each industry. Additionally, public or semi-public institutions may experience an equivalent attack as being less critical simply because they are not in competition with other providers.

Against the threat of ransomware, a vigilant security posture is vital

Our hypothesis that there is a relationship between organizational security posture and attack severity was supported. Most specifically, a weak security posture leads to a preponderance of very severe attacks. This suggests that the attacks were detected late, handled badly, or inadequately isolated. Although this observation is relevant to any type of cybercrime, successful ransomware attacks entail unique and rather devastating consequences such as disabled systems, encrypted data and, subsequently, halted business operations. A security weakness that could be easily fixed might cause substantial damage to the victim and even bankruptcy. For example, LogOrgD was infected via a server vulnerability that was widely documented by academics, security vendors and government bodies. Subsequently, the organization lost access to all critical data, including backups. The victim was rapidly losing its customer base and the business was close to bankruptcy. The business owner was particularly distressed and at some point, even had suicidal thoughts – a lifetime of hard work was about to turn into ashes. Ultimately, the company managed to survive but the recovery was timely, costly and extremely challenging. Therefore, IT/Security professionals must be extremely vigilant when it comes to protecting their organizations against ransomware. 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 [8]. As an IT/Security Manager from LawEnfJ puts it:

> You have to have the fundamentals in place. If you are talking about backups after the event, you are dead in the water. You must have your system set up in a way that actively thwarts these attacks. If you are playing catch-up, then I am sorry, but the game is over at that point. You must stay up-to-date. If you are not staying current in the industry, you are going to get in trouble really quick.

Several respondents commented that if vulnerabilities are not closed down following ransomware attacks, organizations will get attacked again. For example, GovSecJ was attacked 4 times within 6 months. Although the IT/Security Manager wrote a report recommending organizational changes, senior management did not act upon it. Subsequently, three more attacks followed.

Though LawEnfM made a decision to implement all appropriate changes following the first ransomware attack, ransomware struck second time during the recovery process, taking advantage of the same vulnerabilities. Since the organization suffered considerably as a result of two consequent attacks, the external IT provider made a decision to pay the ransom as they felt responsible. Following this devastating experience (two attacks within 2 weeks), LawEnfM made several important changes in its approach to cybersecurity. HealthSerJU had to experience two very severe attacks before senior management realized the importance of security controls and measures:

> I think both attacks fundamentally came down to the fact that there was an under-appreciation of the importance of IT and, therefore, the focus on ensuring that those systems were properly protected was not there .... If we wanted to take a positive from the attacks, it would be that finally executive management gave IT a profile that it has never had before. (IT/Security Manager, HealthSerJU)

Within our sample, public organizations had considerably stronger security postures than those in the private sector. Totally, 78% of the private organizations that we looked at had weak security postures, as opposed to 38% in the public sector. This may be because public institutions have a stronger regulatory mandate to have IT security policies in place. In the UK, the Cyber Essentials scheme was introduced in 2014 and is required for all central government contracts [48]. In contrast, in the private sector, the majority of organizations do not mandate their suppliers to have cybersecurity standards in operation [4].

Of course, the promotion of security standards is one matter, adoption is another and actual compliance yet another again. In the past 12 months, 17 452 Cyber Essentials certificates were issued by the UK government [49] which, going by the estimated 2.6 million businesses in the country [50] represents just 0.7% of the population. Within higher education institutions – from which division 29% of our public sector sample was drawn – there has been considerable resistance to the uptake of the Cyber Essentials standard [51]. The ISO27001 standard has been more widely adopted in the UK, but less so in public administration and educational organizations than elsewhere [52]. The annual UK Cyber Breaches Surveys of recent years reveal that a growing number of businesses are adopting Cyber Essentials, ISO27001, or other similar policies, but it still remains at about half who have no such measures in place [4].

Ransomware attacks, even of the less sophisticated type, can wreak havoc

There was no pronounced effect of the crypto-ransomware propagation class upon attack impact in the sample examined in this study. This is an interesting finding because Generation III crypto-ransomware has the ability to propagate across large networks and completely paralyse organizational operations. As a Detective Sergeant from CyberTR pointed out:

> When I first started, the virus was very specific to the machine. The machine that clicked on the email was the machine that got the virus and the ransomware and that was it. More recent variants of ransomware have the ability to spread. There is definitely a distinction between ransomware that will hit a computer and encrypt any physically connected devices such as USBs, storage

> devices, and it is a lot more simple, and the likes of WannaCry that will travel across networks and spread to all computers. We have seen this evolution, where suspects are using vulnerabilities to spread across networks. This type of ransomware is more prevalent than it ever was because it gives hackers an advantage.

Rationally, Generation III should bring more devastation. However, our data show otherwise. For example, SecOrgM was infected with the less sophisticated Generation II crypto-ransomware. The victim declared bankruptcy shortly after the attack because the organization did not have backups, could not operate without hijacked data and at the same time was not able to meet ransom demands. Similarly, GovSecJN was hit with the Generation II ransomware class but it had a detrimental effect on the victim. Although GovSecJN recovered relatively quickly, data critical to high priority functions was encrypted, affecting essential functions of the organization. Such organizations provide vital services to the local community and many people depend on these services.

On the contrary, EducInstFB was attacked with Generation III crypto-ransomware that infected hundreds of devices. EducInstFB and its staff lost access to an enormous volume of data, which had scientific value. Several critical systems were disabled that stopped the victim from performing their normal daily tasks. The management made a decision to pay the ransom. Although the recovery was lengthy and challenging, EducInstFB eventually repaired its systems and recovered the majority of data. Another victim of Generation III crypto-ransomware – HealthSerJU – was attacked twice and on both occasions over a thousand devices were infected. Although these attacks had a significant negative effect on the delivery of services, HealthSerJU had effective backups and, therefore, promptly restored its systems. EducOrgA was also infected with Generation III crypto-ransomware, affecting the whole network. However, due to the nature of its business, EducOrgA continued its work as a primary school and teaching activities were not interrupted (while administrative data were gradually restored).

Following these observations, we concluded that the crypto-ransomware propagation class alone may not have a direct impact on the consequences of these attacks. Rather, a combination of factors (e.g. the nature of business, availability of resources to recover data or pay the ransom, the type of systems affected, level of preparedness, etc.) are at play.

Beware the 'weakest link'

Although Hypothesis 2c was rejected, indicating that the severity of a ransomware attack is not influenced by the attack target (i.e. human or machine), we observed that organizations with a weak posture were much more likely to be targeted via machine vulnerabilities as a point of entry, whereas those with medium or strong security postures were more likely to be attacked via social engineering tricks. This finding could be explained by the fact that many of our study participants trust that technical controls provide an adequate defence against cyberthreats, which is also a commonly accepted belief among industry professionals. Consequently, IT/Security professionals focus on implementing measures like e-mail hygiene, vulnerability and upgrade management and sophisticated monitoring and detection systems, but seemed to neglect the 'human factor' problem and do not have strong security education and training, the importance of which as a security countermeasure is well established [6, 37, 38]. Therefore, these organizations are attacked via 'the weakest link' – they may have an adequate defence from a technical perspective, but weak employee security practices. As the IT/Security Manager from GovSecJ put it:

> Effective defence always starts with a user. You need to make sure that along with teaching people how to use your applications, IT systems, you incorporate in there a good amount of cyber security.

In our sample, 27 attacks were successful due to humans opening malicious attachments or clicking on links. Several respondents alluded to shortcomings regarding human error and made appropriate changes. For example, LawEnfM replaced online security training with face-to-face tuition after an employee failed to notice rather obvious signs of a malicious e-mail. A staff member from LawEnfJU shut down their own machine after receiving a ransom note and booted several other machines using their credentials. Although the employee hoped to solve the problem, they instead infected more machines and lost precious time to contain infection. Since then, LawEnfJU implemented a new policy that obliges employees to report any out-of-ordinary activity, no matter how insignificant it seems. The organization regularly sends its employees 'call and verify' warnings to remind them of this new rule. However, even with effective security education in place, humans are continually prone to make mistakes and do things they know they probably shouldn't. For example, an employee from GovSecJN who had recently completed security training still proceeded to open an e-mail attachment, even though he felt it was quite suspicious and potentially risky.

Don't become an easy target, be careful what you reveal about your organization

Targeted attacks were more likely than opportunistic ones to lead to severe consequences in the observed sample. This result is expected as targeted attacks require a lot of preparation, but the 'prize' is much higher:

> There is a recent trend of a particular variant of ransomware called BitPaymer, which is seen as a big problem. It seems to me to be very targeted because cybercriminals are making extremely large demands on the businesses, which I have never seen before – £30,000 –so they are clearly very targeted. Cybercriminals know the targets they are going after. (Detective Sergeant, CyberTL)

> Such attacks suggest that there is some kind of network reconnaissance behind, so cybercriminals know what company they are targeting and how much to ask for. Cybercriminals will say, 'Wait there, your turnover is £400m so you can pay maybe £2m'. There are victims out there that have paid up to £1,000,000 or even more to get the decryption key. (Detective Constable, CyberBR)

Clearly, such extravagant amounts would have a more severe effect on an organization than, e.g. the typical £300–500 ransom. In our own sample, one small IT company (VirtOrgD) was asked to pay 75 bitcoins (approximate value £352 000 at the time of the attack), a ransom amount the victim could not afford to pay. After intense negotiations, hackers agreed to reduce the ransom amount to 65 bitcoins, but it was still too high for VirtOrgD. The victim had no choice but to recover from partial backups. In the first stages of recovery the management was not sure if the business was going to survive this attack as the VirtOrgD was rapidly losing its customer base. Through tremendous efforts of staff and with the help of external specialists, VirtOrgD managed to restore its business, although, inevitably, some substantial losses occurred. Similarly, another company (ITOrgJL) was asked to pay 100 bitcoins (approximate value of £470 000 at the time of the attack). ITOrgJL was able to negotiate the ransom down to 15 bitcoins and effectively recovered with a decryption key provided by hackers.

Both organizations VirtOrgD and ITOrgJL had weak security postures, which allowed hackers not only to penetrate their networks but also stay undetected for several days searching for loopholes to spread within the network and encrypt multiple devices, including servers that contained crucial data and systems. This confirms our observation that the majority of targeted attacks were executed against organizations that had weak security posture. The lethality of targeted attacks lies within hackers' ability to execute network reconnaissance in order to find the most critical company's assets (e.g. backup server, customer data, etc.) and security weaknesses that will allow to hijack these assets. It is up to organizations to take appropriate measures to avoid such dramatic consequences.

Conclusions

Our research findings demonstrate that several factors, including 'organization sector', 'security posture' and 'attack type', influence the degree of severity of ransomware attacks. More specifically, within our sample, private organizations were more likely to experience severe consequences compared to public ones. Interestingly, public organizations investigated in this study had considerably stronger security postures than those in the private sector. Private organizations typically operate to generate profit and any interruptions to services can cause grave damage to them. Public organizations, on the contrary, are funded by the government to serve the public. Subsequently, financial implications are not always relevant to them. We assert that private organizations need to recognize this vulnerability and 'up their game' in the security realm.

Furthermore, organizations that had weak security postures suffered harsher outcomes of ransomware attacks as opposed to companies with stronger postures. This finding indicates that the need to strengthen security postures in a bid to defend organizational assets against ransomware attacks is greater than ever. Hackers are relentlessly taking advantage of well-documented issues (e.g. RDP bruteforce, poor security training, insufficient vulnerability management). It is important to note that organizations must focus on technical and non-technical controls as both are vital; one without the other is futile. As our results demonstrate, targeted attacks are mainly preying on technical shortcomings but even if all technical loopholes are closed down, hackers can still hit a potential victim by exploiting human weaknesses.

Moreover, targeted attacks brought more devastation to affected organizations in our sample compared to those who were hit opportunistically. Offenders normally invest more effort into targeted attacks and hence, expect higher yields. For example, a thorough investigation of the target may take place, so the hackers can understand how profitable the business is, what information is critical to its continuity and how much the victim can potentially afford to pay. Whether or not the victim pays, they are still going to suffer substantially. In a scenario where they pay, the ransom is going to be very high and the organization is going to experience considerable financial losses. In a situation where the victim does not pay, they are going to suffer not only financially (in many cases, recovery is more expensive than the ransom payment), but also experience significant disruptions to business operations. Therefore, it is worth making cybersecurity investments rather than face consequences of the targeted ransomware attacks. As our findings suggest, organizations with stronger security postures are less vulnerable to targeted attacks.

Our results also indicate that 'organization size', 'crypto-ransomware propagation class' and 'attack target' have no significant impact on the severity level of ransomware attacks. Within our sample, organizations of all sizes were afflicted by ransomware attacks, with consequences ranging from less severe (e.g. relatively short business continuity disruption timeline and insignificant information loss) to highly severe, where organizations faced a challenging recovery and, in many cases, came very close to business bankruptcy. In fact, one organization in our sample (SecOrgM) did not survive the ransomware attack. This finding underlines the indiscriminate nature of ransomware and serves as caution against common but dangerous attitudes such as 'hackers could not possibly gain anything from attacking us – we are too small', 'we do not hold any state secrets or any other sensitive information that would be of interest to hackers', 'hackers are normally after banks as this is where the money is', etc.

Since 2013, ransomware has evolved considerably and become much more technically advanced and dangerous. Generation III is substantially more of a menace than Generation II because of its greater degree of contagiousness and ability to self-propagate across infected networks. However, we found that the propagation class of crypto-ransomware by itself had no effect on the severity of crypto-ransomware attacks in the observed sample. Regarding the attack target (i.e. machine vs. human), crypto-ransomware equally impacts victims despite the network access method.

As ransomware attacks continue to hurt businesses around the globe, our results convey several important messages. First, we urge organizations of all sizes, small, medium and large, to strengthen their security posture. Secondly, we specifically stress that the vulnerabilities of private companies to ransomware attacks must be realized and addressed. Offenders are aware of their dependency on data and systems and take advantage of it. Thirdly, we conclude that the strength of ransomware is not in its technical capabilities and rapid evolution; rather, it lies within relentlessness of hackers who are persistently searching for a range of weaknesses within organizations. Security holes are widely exploited by perpetrators, but hackers also understand the sentimental value organizations may have to their owners who possibly spent a lifetime building their business (e.g. LogOrgD case). Criminals exploit the sense of responsibility that IT and Cyber Security professionals may experience if a company is significantly suffering from an attack (e.g. LawEnfM), or the responsibility management may feel because their staff is facing very challenging working conditions during attacks and potential harsh consequences post-attacks (e.g. EducInstFB). All of these factors inevitably make ransomware attacks ever so painful, while hackers are persistently doing their homework on potential victims; and this is why targeted attacks hit even harder.

This work makes a number of valuable contributions to the existing body of academic literature on ransomware. It increases knowledge about factors that can make crypto-ransomware attacks absolutely unbearable for affected organizations. We urge readers to learn from the experiences of victims presented in this work and take appropriate preventative actions to avoid, transfer or mitigate the risks of a crypto-ransomware attack. The article also introduces (see 'Crypto-ransomware propagation class' section) a simple but useful set of terms that can be used by various parties (e.g. academics, industry professionals, government bodies, etc.) to refer to different classes of this threat according to the degree of infectiousness, i.e. 'Generation I', 'Generation II', etc. Finally, we developed an Impact Assessment Instrument, which can be applied in further academic works that specifically focus on the crypto-ransomware impact.

This study has a number of limitations. As always, studying cybercrime is a challenge because researchers are faced with incomplete data, skewed surveys and questionable assumptions. The majority of our respondents were based in one country (the UK). Our sample size

of 55, though respectable, is still quite small. Therefore, statistically speaking, the findings cannot be generalized outside the given sample and are only applicable within the observed 55 ransomware attacks. A logical follow-on would be to test our conclusions against a larger, more international data set – but a practical problem is how to readily obtain such data. Typically, ransomware victims do not disclose the full reality of their experiences in official complaints or incident reports [3]. Insurance companies such as Advisen have databases of incidents, but these only include organizations that were insured against cyberattacks and made claims. Unfortunately, these sorts of sampling and access issues are typical in cybersecurity research [25] and, as we earlier saw in Table 1, it greatly complicates comparability between studies. We executed our study as rigorously as we could, combining quantitative and qualitative data, and although we believe it is robust and broadly generalizable, that is a point of conjecture.

Furthermore, in terms of limitations, in Phase 1, we interviewed one participant per organization. This is a very common limitation in qualitative data collection, where the principal interviewee typically plays the role of a 'gatekeeper', especially when the subject matter pertains to highly sensitive and confidential matters within the organization. We used a snowballing sampling strategy in Phase 2 of data collection which, though not ideal, was the only pragmatic way we could collect data on ransomware attacks.

As regard future research, in the next step we are planning to learn what makes ransomware so effective in a wider cybercrime eco-system. While in this study we assessed factors that make these attacks impactful, ransomware is a very complex threat and organized criminals employ various tactics to make these attacks successful. Therefore, we intend to learn about numerous vulnerabilities that cybercriminals prey on (whether technical, social or psychological), specifically focusing on victims' decision-making processes regarding ransom payments. The ultimate purpose of this study will be to identify a series of measures that could potentially reduce ransom payments.

Acknowledgements

We would like to extend our sincere gratitude to all study participants for their invaluable contribution to this research. We greatly appreciate interviewees' time and genuine effort. We realize 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. It is very important that other organizations learn from your experiences. Special thanks to Robert McArdle, the Director of Cybercrime Research Team at Trend Micro, who provided expert advice on technical measures against crypto-ransomware attacks. We would like to acknowledge the relentless commitment of police officers from UK Regional Cybercrime Units in providing data and advising on study results. 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.

Funding

This work was supported by the Engineering and Physical Sciences Research Council [EP/P011721/1].

References

1. Europol. *Internet Organised Crime Threat Assessment*, 2020. https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
2. Sophos. *The State of Ransomware 2020: Results of an independent survey across 26 countries*, 2020. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
3. FBI. *2019 Internet Crime Report*, 2020. https://pdf.ic3.gov/2019_IC3Report.pdf [Accessed January 2020]
4. UK Government. *Cyber Security Breaches Survey 2020*, 2020. https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020
5. Simoiu C, Gates C, Bonneau J, *et al.* "I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In: *Proceedings of USENIX Symposium on Usable Privacy and Security (SOUPS)*, Santa Clara, CA, 11–13 August 2019.
6. Connolly LY, Lang M, Gathegi J, *et al.* Organisational culture, procedural countermeasures, and employee security behaviour: a qualitative study. *Inf Comp Secur* 2017;**25**:118–36.
7. Richardson R, North M. Ransomware: evolution, mitigation and prevention. *Int Manage Rev* 2017;**13**:10–21.
8. Connolly L, Wall SD. The rise of crypto-ransomware in a changing cybercrime landscape: taxonomising countermeasures. *Comput Secur* 2019;**87**:1–18.
9. Holt T, Bossler A. An assessment of the current state of cybercrime scholarship. *Deviant Behav* 2014;**35**:20–40.
10. Rege A. Incorporating the human element in anticipatory and dynamic cyber defense. In: *Proceedings of the 2016 IEEE International Conference on Cybercrime and Computer Forensic*, Vancouver, BC, 12–14 June 2016, 1–7.
11. Connolly L, Borrion H. Your money or your business: Decision-making processes in ransomware attacks. In: *Proceedings of 2020 International Conference in Information Systems*. Association for Information Systems, 14–16 December 2020.
12. Payne BK, Hawkins B, Xin C. Using labelling theory as a guide to examine the patterns, characteristics, and sanctions given to cybercrimes. *Am J Crim Justice* 2019;**44**:230–47.
13. Maimon D, Louderback E. Cyber-dependent crimes: an interdisciplinary review. *Annu Rev Criminol* 2019;**2**:191–216.
14. Atapour-Abarghouei A, Bonner S, McGough AS. Volenti non fit injuria: ransomware and its victims. In: *2019 IEEE International Conference on Big Data*, IEEE, December 2019, 4701–7.
15. Choi KS, Scott TM, LeClair DP. Ransomware against police: diagnosis of risk factors via application of cyber-routing activities theory. *Int J Forensic Sci Pathol* 2016;**4**:253–8.
16. Zhao JY, Kessler EG, Yu J, *et al.* Impact of trauma hospital ransomware attack on surgical residency training. *J Surg Res* 2018;**232**:389–97.
17. Zhang-Kennedy L, Assal H, Rocheleau J, *et al.* The aftermath of a crypto-ransomware attack at a large academic institution. In: *Proceedings of the 27th USENIX Security Symposium*. Baltimore, MD, 15–17 August 2018, 1061–78. ISBN 978-1-939133-04-5.
18. Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science* 2019;**8**:2–22.
19. Shinde R, Van der Veeken P, Van Schooten S, *et al.* Ransomware: studying transfer and mitigation. In: *Proceedings of the 2016 International Conference on Computing, Analytics and Security Trends (CAST)*. Pune: IEEE, 19–21 December 2016, 90–5.
20. Ioanid A, Scarlat C, Militaru G. The effect of cybercrime on Romanian SMEs in the context of wannacry ransomware attacks. In: *Proceedings of the European Conference on Innovation and Entrepreneurship*, Paris: Academic Conferences International Limited, 21–22 September 2017, 307–13.
21. Byrne D, Thorpe C. Jigsaw: an investigation and countermeasure for ransomware attacks. In: *Proceedings of the European Conference on Cyber Warfare and Security*. Dublin: Academic Conferences International Limited, 29–30 June 2017, 656–65.
22. Riglietti G. Cyber security talks: a content analysis of online discussions on ransomware. *Cyber Secur* 2017;**1**:156–64.
23. Agustina JR. Understanding cyber victimization: digital architectures and the disinhibition effect. *Int J Cyber Criminol* 2015;**9**:35–54.
24. Ngo FT, Paternoster R. Cybercrime victimization: an examination of Individual and situational level factors. *Int J Cyber Criminol* 2011;**5**:773–93.
25. Furnell S, Emm D, Papadaki M. The challenge of measuring cyber-dependent crimes. *Comput Fraud Secur* 2015;**2015**:5–12.

26. Business Continuity Institute [BCI]. *BCI Cyber Resilience Report*. Business Continuity Institute, 2018.
27. Beazley. *Breach Briefing*, 2019. https://www.beazley.com/Documents/2019/beazley-breach-briefing-2019.pdf
28. Al-Rimy BAS, Maarof MA, Shaid SZM. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. *Comput Secur* 2018;**74**:144–66.
29. Mansfield-Devine S. Securing small and medium-size businesses. *Network Secur* 2016;**2016**:14–20.
30. Renaud K. How smaller businesses struggle with security advice. *Comput Fraud Secur* 2016;**2016**:10–18.
31. Browne S, Lang M, Golden W. Linking threat avoidance and security adoption: a theoretical model for SMEs. *BLED 2015 Proceedings*, 2015, 35. http://aisel.aisnet.org/bled2015/35
32. Smith R. Ransomware is indiscriminate – secure your systems now, *Petri*, June 7, 2017. https://www.petri.com/ransomware-indiscriminate-secure-systems-now
33. Kurpjuhn T. The SME security challenge. *Comput Fraud Sec* 2015;**2015**:5–7.
34. Bergmann MC, Dreißigacker D, Skarczinski B, *et al*. Cyber-dependent crime victimization: the same risk for everyone? *Cyberpsychol Behav Soc Network* 2018;**21**:84–90.
35. Parkinson S. Are public sector organisations more at risk from cyber-attacks on old computers?, *The Conversation*, 16 May 2017. https://theconversation.com/are-public-sector-organisations-more-at-risk-from-cyber-attacks-on-old-computers-77802
36. NIST. *Guide for Conducting Risk Assessments, Information Security, NIST Special Publication 800-30*. National Institute of Standards and Technology, Gaithersburg, MD, 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
37. Connolly L, Lang M, Wall DS. Information security behavior: a cross-cultural comparison of employees in Ireland and United States. *Inf Syst Manage* 2019;**36**:306–22.
38. Connolly L, Lang M, Tygar JD. Employee security behaviour: the importance of education and policies in organisational settings. In: Paspallis N, Raspopulos M, Barry C, *et al*. (eds.), *Advances in Information Systems Development Methods, Tools and Management. Lecture Notes in Information Systems and Organisation*. Springer: New York, 2018: 79–96.
39. Brewer R. Ransomware attacks: detection, prevention and cure. *Network Secur* 2016;**2016**:5–9.
40. Connolly L, Wall SD. Hackers are making personalised ransomware to target the most profitable and vulnerable, *The Conversation*, 2019. https://theconversation.com/hackers-are-making-personalised-ransomware-to-target-the-most-profitable-and-vulnerable-113583
41. Williams M. 10 disturbing facts about employees and cyber security, *Pensar*, 13 December 2018. https://www.pensar.co.uk/blog/infographic-10-disturbing-facts-about-employees-and-cyber-security
42. Browne S, Lang M, Golden W. The insider threat - understanding the aberrant thinking of the rogue 'Trusted Agent'. In: *Proceedings of European Conference on Information Systems*, Münster, Germany, 26–29 May 2015.
43. Creswell JW, Plano Clark VL. *Designing and Conducting Mixed Methods Research*, 2nd edn. Thousand Oaks, CA: Sage Publications, 2011.
44. Eisenhardt KM. Building theories from case study research. *Acad Manage Rev* 1989;**14**:532–50.
45. Zumbo BD, Gadermann AM, Zeisser C. Ordinal versions of coefficients alpha and theta for Likert rating scales. *J Mod Appl Stat Meth* 2007;**6**:21–9.
46. Eurostat. Your key European statistics, *Eurostat*, 2020. https://ec.europa.eu/eurostat/web/structural-business-statistics/structural-business-statistics/sme
47. Porcedda MG, Wall DS. Cascade and chain effects in big data cybercrime: lessons from the TalkTalk hack. In: *Proceedings of WACCO 2019: 1st Workshop on Attackers and Cyber-Crime Operations*, IEEE EuroS&P 2019, Stockholm, 20 June 2019.
48. UK Government. *Procurement Policy Note 09/14: Cyber Essentials Scheme Certification*, 2014. https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification
49. UK National Cyber Security Centre: Certificate Search. https://www.ncsc.gov.uk/cyberessentials/search
50. Eurostat, 2020b. https://ec.europa.eu/eurostat/tgm/table.do? tab=table&init=1&language=en&pcode=tin00170&plugin=1
51. Chapman J, Chinnaswamy A, Garcia-Perez A. The severity of cyber attacks on education and research institutions: a function of their security posture. In: *Proceedings of ICCWS 2018 13th International Conference on Cyber Warfare and Security*. Academic Conferences and Publishing Limited, 2018, 111–9.
52. ISO. ISO Survey, 2019. https://www.iso.org/the-iso-survey.html

Appendix 1: Profile of participant organizations and corresponding attacks characteristics

Attack ID	Crypto-ransomware propagation class; attack target; attack type	Organization alias	Industry; size; sector
1	Generation II; human; opportunistic	LawEnfJ	Law enforcement; SME; public
2	Generation II; human; opportunistic	GovSecJN	Government; large; public
3	Generation II; machine; opportunistic	GovSecJ	Government; large; public
4	Generation II; human; opportunistic		
5	Generation II; machine; opportunistic		
6	Generation II; machine; opportunistic		
7	Generation II; machine; opportunistic	EducInstF	Education; large; public
8	Generation III.a; machine; targeted	EducInstFB	Education; large; public
9	Generation II; human; opportunistic	LawEnfM	Law enforcement; SME; public
10	Generation II; human; opportunistic		
11	Generation III.a; machine; targeted	GovSecA	Government; large; public
12	Generation II; human; opportunistic	LawEnfJU	Law enforcement; SME; public
13	Generation III.b; machine; opportunistic	HealthSerJU	Health service; large; public
14	Generation III.a; human; targeted		
15	Generation II; human; opportunistic	LawEnfF	Law enforcement; SME; public
16	Generation II; machine; opportunistic	ITOrgA	IT; SME; private
17	Generation III.a; machine; opportunistic	ConstrSupA	Construction; SME; private
18	Generation III.a; machine; targeted	EducOrgA	Education; SME; public
19	Generation II; human; opportunistic	SecOrgM	IT; SME; private
20	Generation III.a; machine; targeted	ITOrgJL	IT; SME; private
21	Generation II; human; opportunistic	CloudProvJL	IT; SME; private
22	Generation III.a; machine; targeted	InfOrgJL	Infrastructure; SME; private
23	Generation III.a; machine; opportunistic	ConstrSupJ	Construction; SME; private
24	Generation II; human; opportunistic	RelOrgJ	Religion; SME; private
25	Generation III.a; machine; targeted	SportClubJ	Entertainment; large; private
26	Generation III.a; machine; targeted	UtilOrgD	Utilities; large; private
27	Generation III.a; e-mail; targeted	VirtOrgD	IT; SME; private
28	Generation III.a; machine; opportunistic	CleanOrgD	Cleaning; SME; private
29	Generation II; human; opportunistic	EducOrgD	Education; SME; public
30	Generation II; human; opportunistic	SerOrgD	Waste; SME; private
31	Generation III.a; machine; opportunistic	EducCompD	Education; SME; public
32	Generation III.a; machine; opportunistic	PrimOrgD	Education; SME; public
33	Generation III.a; machine; opportunistic	LogOrgD	Logistics; SME; private
34	Generation III.a; machine; opportunistic	ITCompD	IT; SME; private
35	Generation III.a; machine; opportunistic	LogWarJ	Logistics; large; private
36	Generation III.a; machine; targeted	TranspOrgJ	Transport; large; private
37	Generation II; human; targeted	CharOrgJ	Charity; SME; public
38	Generation II; human; opportunistic	EducInstJ	Education; large; public
39	Generation II; human; opportunistic	DigMedM	Retailer; SME; private
40	Generation II; human; opportunistic	ConstrSupAP	Construction; SME; private
41	Generation II; human; opportunistic	FinOrgAP	Finance; SME; private
42	Generation II; unknown; unknown	ConstrOrgAP	Construction; SME; private
43	Generation II; unknown; unknown	LetAgenAP	Letting agency; SME; private
44	Generation III.a; machine; targeted	EducOrgAP	Education; large; public
45	Generation II; human; opportunistic	ConstrArcAP	Construction; SME; private
46	Generation II; human; opportunistic	LegalOrgAP	Legal; SME; private
47	Generation II; human; opportunistic	BevOrgAP	Beverages; SME; private
48	Generation II; human; opportunistic	ChCarAP	Childcare; SME; public
49	Generation III.a; machine; opportunistic	EducPrimAP	Education; large; public
50	Generation II; human; opportunistic	RetOrgAP	Retailer; large; private
51	Generation III.a; machine; opportunistic		
52	Generation III.a; machine; targeted	ITOrgAP	IT; SME; private
53	Generation III.a; machine; opportunistic	MarkOrgAP	Marketing; SME; private
54	Generation III.a; machine; opportunistic	ChemOrgAP	Chemical; SME; private
55	Generation III.a; machine; opportunistic	EducHscAP	Education; large; public
56	Generation III.a; machine; opportunistic	HospOrgAP	Hospitality; large; private
57	Generation II; human; opportunistic	WasteOrgAP	Waste; SME; private
58	Generation III.a; machine; opportunistic	FinCompAP	Finance; large; private
59	Generation II; human; targeted	LegAdvAP	Legal; SME; private
60	Generation III.a; machine; opportunistic	LegSolcAP	Legal; SME; private

Appendix 2: Sample interview questions (Phase 1)

Questions
Can you please tell me about the attack?
How would you rate the attack in terms of the level of severity?
Was your business affected by the ransomware attack?
If yes, then to what extent?
What functions were affected?
Were your data affected by the ransomware attack?
If yes, then to what extent?
Did you manage to restore the data that were encrypted?
In your opinion, are there any other negative impacts the ransomware attack had on your organization?
In your opinion, was the ransomware attack effective?
If yes, why do you think ransomware was effective?
What factors contributed to the effectiveness of this attack?

Appendix 3: Impact assessment exercise exemplar

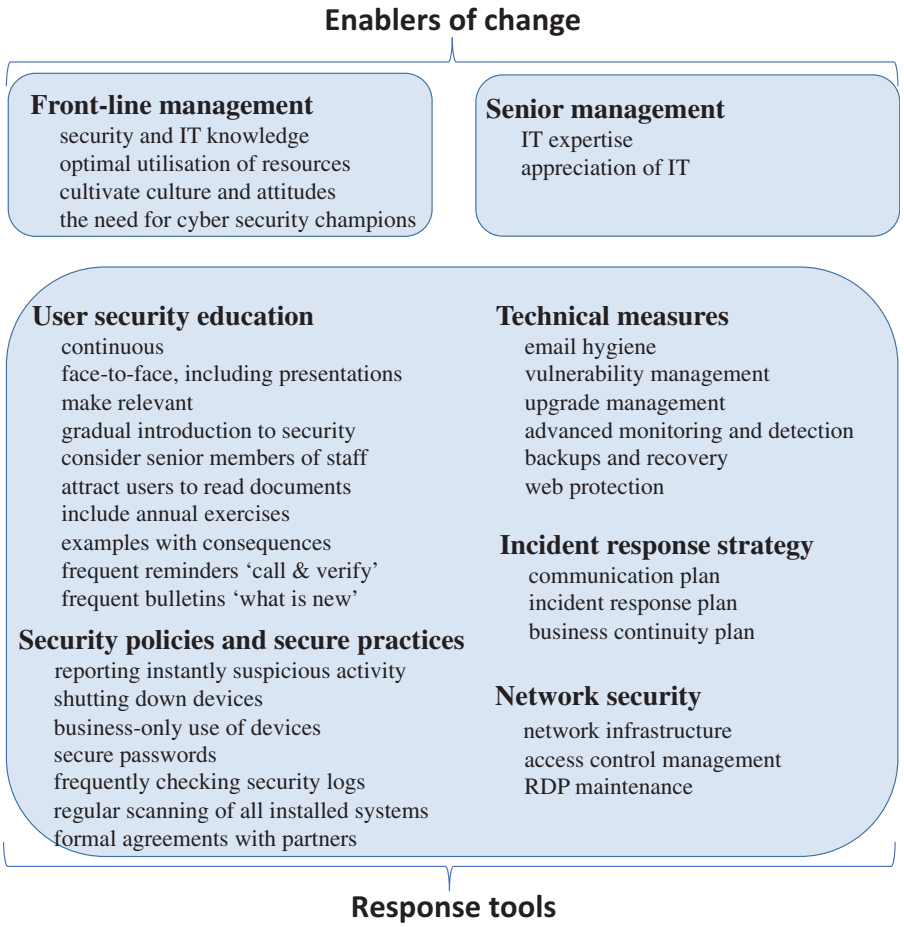
Crypto attacks	Category	Item → corresponding impact level → corresponding digit
Attack 1	Business continuity disruption timeframe	Up to 1 week → 'Low' → 1
	Encrypted information critical to business	Not critical → 'Low' → 1
	Information loss	Some loss acceptable with incremental backups → 'Low' → 1
	Affected devices	One desktop and shares on a server → 'Low' → 1
	Recovery time	Up to 2 weeks → 'Low' → 1
Maximum value	1	
Attack impact level	Low	
Attack 9	Business continuity disruption timeframe	Up to 1 week → 'Low' → 1
	Encrypted information critical to business	Critical to high priority functions → 'High' → 3
	Information loss	Some loss acceptable with incremental backups → 'Low' → 1
	Affected devices	Several desktops and shares on servers → 'Low' → 1
	Recovery time	Up to 1 month → 'Medium' → 2
Maximum value	3	
Attack impact level	High	

Appendix 4: Sample interview questions (Phase 2)

Questions
Can you please comment on the volume of infection spread?
Did ransomware take advantage of the local user security context and only encrypted server shares?
Or did it spread across network, taking advantage of software vulnerabilities or weak admin passwords?
Did disruption to business continuity last for:
Up to 1 week
Up to 2 month
Several months or more
How much information was lost as a result of this attack?
No loss or some loss acceptable with incremental backups
Information loss affecting some critical business functions
Information loss affecting majority or all critical business functions
In your expert opinion, what was the severity of the consequence of this attack on victim organization ('Low', 'Medium', 'High')?
Why do you think so?

Appendix 5: Criteria used to assess the security posture of organizations

The assessment of the security posture of organizations was informed by a careful consideration of the organization's level of preparedness across a range of criteria, as shown in the taxonomy below (based on Connolly and Wall [8]).



Appendix 6: Security posture exemplars

Strong Security Posture: LawEnfJ had partnerships with other organizations, which involved sharing some systems including e-mail. An employee received a malicious e-mail into the external partner's inbox and opened it on the machine belonging to LawEnfJ, infecting the network. An investigation revealed that the partner-organization did not have appropriate e-mail hygiene that could have stopped this e-mail from entering the inbox. Nevertheless, LawEnfJ had an acute awareness of the ransomware threat and abundant knowledge on how to prevent and mitigate ransomware attacks. When the ransomware hit, the organization responded timely and methodically. All systems and data were recovered over one weekend. Some data were lost as part of the incremental backups practice, which is an acceptable industry practice. Following the attack, LawEnfJ instigated a formal agreement with all external partners on minimal security measures that they must implement.

Medium Security Posture: GovSecJN had multiple layers of security controls to protect its business from cyberthreats. However, when the ransomware attack took place, GovSecJN realized that some controls were not equipped to deal with the incident. For example, a communication plan did not consider the fact that crypto-ransomware has the ability to encrypt systems, including e-mail, stripping organizations of the most common communication methods; business continuity plans did not take into consideration the loss of IT. Although all systems and data were restored in 1 week (from backups), some critical services were unavailable for several days, inevitably affecting customers and staff. Following the attack, GovSecJN implemented several changes, including updated communication and business continuity plans.

Weak Security Posture: EducInstFB had several serious network oversights (e.g. the lack of network visibility, a flat network structure, poor access control management, poor security practices, ineffective backups) that led to severe consequences, where crypto-ransomware infected the whole network comprised hundreds of devices. Subsequently, many vital systems became unresponsive, crippling important business functions. A large amount of data would have been lost as a result of this attack if the organization had not paid the ransom. The recovery process was very challenging and lasted for months.

Appendix 7: Profile of organizations