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.

In recent years, Europol’s annual Internet Organized 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 organizations within as well as outside Europe’. Furthermore, as starkly evidenced by an international survey of 5000 IT managers, the incidence of ransomware attacks is growing exponentially. Similar trends have been observed by government and law enforcement bodies. 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.

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. 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. 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 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, the victim and the crime itself. 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.

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

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 proposes several behavioral and environmental factors that should, in theory at least, elevate the risk of being victimized. In practice, however, as found by Ngo and Paternoster, 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 ransomware attacks; secondly, our focus is not on individual victims, but rather on organizations.

Although several reports 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. Statistics about the incidence of ransomware attacks vary wildly. In an international study based on 574 participants across 77 countries, BCI 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. Simoiu et al. estimated that about 2–3% of their sample of 1180 American adults were hit by ransomware between 2016 and 2017. Similarly, Ioanid et al. 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. found that as many as 61% of UK respondents had experienced at least one attack, and Shinde et al. 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. 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. 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 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.

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 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 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. SMEs, by their entrepreneurial nature, are more likely to engage in risk-taking behavior. 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 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 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. 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:

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 . 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. In view of the differences between public and private sector organizations, we put forward the following hypothesis:

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’. 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. 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. Connolly and Wall 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 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. In their studies of ransomware victims, Shinde et al. and Zhang-Kennedy et al. 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 behavior.

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:

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. 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 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:

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 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. Therefore, the consequences of targeted attacks are potentially more severe Accordingly, we form this hypothesis:

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 Since numerous sources allocate a lot of blame to human error and claim that human mistakes cost organizations huge amounts of money , 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:

The attack target, i.e. human or machine, influences the impact severity of a ransomware attack

This study used a mixed methods approach following an exploratory sequential design . 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 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 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

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 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

An inductive content analysis method was used to analyze 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 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 organization 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 to test for internal reliability. The value for ordinal α = 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’.

Next, using the Impact Assessment Instrument shown in Table 3, we analyzed 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

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

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

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 sub-sample 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 = 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.

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 brute-force, 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. 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

today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in every day life. In today’s technical environment many latest technologies are changing the face of the man kind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Today more than 60percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc. also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man’s language cyber crime may be defined as crime committed using a computer and the internet to steel a person’s identity or sell contraband or stalk victims or disrupt operations with malevolent

There will be new attacks on Android operating system based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cybersecurity, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read if. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks(e.g. the Internet, e-commerce),mobile telephones, wireless microphones, wireless intercoms. Hence by encrypting the code one can know if there is any leakage of information

Buffer overflows have been the most common form of security vulnerability for the last ten years. More over, buffer overflow vulnerabilities dominate the area of remote network penetration vulnerabilities, where an anonymous Inter-net user seeks to gain partial or total control of a host. If buffer overflow vulnerabilities could be effectively eliminated, a very large portion of the most serious security threats would also be eliminated. In this paper, we survey the various types of buffer overflow vulnerabilities and attacks, and survey the various defensive measures that mitigate buffer overflow vulnerabilities, including our own Stack Guard method. We then consider which combinations of techniques can eliminate the problem of buffer overflow vulnerabilities, while preserving the functionality and performance of existing systems. Buffer overflows have been the most common form of security vulnerability in the last ten years. Moreover, buffer overflow vulnerabilities dominate in the area of remote network penetration vulnerabilities, where an anonymous Internet user seeks to gain partial or total control of a host. Because these kinds of attacks enable anyone to take total control of a host, they represent one of the most serious classes security threats. For instance, among the five “new” “remote to local” attacks used in the 1998 Lincoln Labs intrusion detection evaluation, three were essentially social engineering attacks that snooped user credentials, and two were buffer overflows. 9 of 13 CERT advisories from1998 involved buffer overflows and at least half of1999 CERT advisories involve buffer overflows

No matter where you currently are on the “return” continuum, some form of accentuated remote work, it seems- it’s here to stay. The days of 30%ish of your workforce remotely accessing your systems sometimes are in the past.

Vast swaths of your workforce will continue outside on prem for the foreseeable future. And so, endpoint security and identity management have found a dovetail moment.

With your systems and your users both being mostly remote threat vectors are innumerable. Locking down endpoint security is table stakes. In fact, our upcoming Mid-Year Report uncovers the fact that Endpoint security went from the fifth highest to the second highest budget spend in the past six months. So that covers the systems and the tools, but what about the people?

Shoving the people through a VPN or RDS or VDI is table stakes. But credential management, third party accountability, handcuffing productivity and yes- access management are all issues.

Access is on or off for my solutions thus more security is needed. That is where and why IAM solutions meet endpoint security.

And there are some IAM solutions that do in fact provide you with the ability to amplify productivity.

Based on your system make-up and technology stack, that plug and play timeline is potentially going to be extensive. On the other side of that implementation though, looks to be a pretty seamless playground of efficiency and productivity for your users.

Budgets aren’t what they used to be- the upcoming Mid-Year Report also shines a light on the fact that most budgets are now flat or downward facing which is the inverse of the direction we were headed just one year ago.

So investment decisions are more delicate than ever. But mindset doesn’t cost you a dime. Give another look at the Venn diagram that now is your endpoint security and access management and please reaffirm your systems, your users and you are all set.

The Center for Internet Security (CIS), founded in 2000, was founded to identify, develop, validate, promote, and sustain best practice solutions for cyber defense. The different areas of focus and programs within the CIS work to crowdsource information for the sake of developing new capabilities for security. The CIS has identified key security controls which Lane buckets into basic, foundational, and organizational.

Within Lane’s client base, he observes that most of his customers are utilizing perimeter and prevention tools; endpoint prevention and firewalls; email security; and recovery plans. While that’s a great start, the goal of an organization should be to continuously allocate resources and capabilities to increase security controls.

Before covering the top six controls, Lane suggests getting a pentest done in order to prioritize which controls get put in and in what order. That said, Lane contends that all a pentest will really tell you is to implement at least the first 6 controls of CIS and may need to be done to validate budget. He actually discourages customers from doing pen tests UNTIL they have implemented basic controls. The order of what controls should be implemented should actually be calculated based on a risk analysis and assessment (which CIS has a CIS RAM to help companies walk through that). Next, Lane covers six of the 20 top CIS controls.

The first control is inventory and control of hardware assets. The second of inventory and control of software assets. These controls involve actively managing all hardware and software on the network so that only authorized software and hardware are installed and can execute, and that all unauthorized and unmanaged software and hardware are found and prevented from installation or execution.  Control three is continuous vulnerability management. An organization must continuously acquire, assess, prioritize, and act on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Control four is the controlled use of administrative privileges. This entails using processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. Control five is securing configuration for hardware and software. This control involves establishing, implementing, and actively managing the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process to prevent attackers to prevent attackers from exploiting vulnerable services and settings. Control six is the maintenance, monitoring, and analysis of audit logs. Collecting, managing, and analyzing audit logs of events helps future detection and recovery from attacks.

The disclosure of ransomware attacks grows as U.S. municipalities and city services – all rich in data – find themselves the target of cyber hijacking. Beyond payment (or not) of the ransom, little has been shared about the cost for an organization to recover from this form of attack. Recent news from three entities is helping shed light on the recovery costs and on-going learnings from ransomware attacks. Hackers successfully infiltrated systems operated by the City of Baltimore this past May. The attackers encrypted data files and demanded a ransom in exchange for the decryption keys. Mayor Bernard C. “Jack” Young refused to pay and IT leaders were instructed to rebuild the municipality’s computer systems. City of Baltimore officials placed a price tag of $18 million on the estimated cost of the ransomware attack. It is unfortunate when a ransomware attack occurs. And it is nearly unfathomable that a second attack would even be a consideration. However, Wolcott Public Schools in Connecticut finds its school district in this predicament. In June of this year, [the school district](https://www.courant.com/news/connecticut/hc-news-cyber-attacks-schools-towns-ransom-20190831-jrkimu7h2fbvneiiungecspq3y-story.html#nt=instory-link) was hit with a ransomware attack. The cyber hijackers requested $12,000 to release the encryption keys though the school board has not been paid it. Reports in the Hartford Courant say that Wolcott Public Schools noticed suspicious activity in the district’s computer systems in early September. Since the district was still recovering services locked out from the June attack, officials [voluntarily shut down the network](https://www.courant.com/news/connecticut/hc-news-wolcott-schools-hacked-computer-systems-20190911-abpqgqwhdzc45p4k36d22k6wce-story.html) out of caution. In March, the city of Albany, New York had its computer systems shut down when a ransomware attack locked its data. Details have not been shared about the ransom amount requested to release the data.

WNYT, an Albany news channel, requested the city [disclose details of expenditures](https://wnyt.com/news/albany-spent-over-300k-recovering-from-cyberattack/5491067/) associated with the ransomware attack. City officials responded with a cost of $161,000 related to employee overtime for re-entering lost data, hardware and software system upgrades, credit monitoring services for city employees and professional cyber security services. The amounts differ from the $300,000 that Mayor Kathy Sheehan shared during an event.

Sheehan said that a municipality such as Albany always has unexpected events. “Sometimes, it's a catastrophic storm, this past year it was an unexpected ransomware attack.” The city has invested to rebuild its former capabilities to deliver services to its citizens and invested to make sure this type of attack does not happen again.

Without a full post-mortem review of actions and best practices available, organizations can still action the security team with information that is known about ransomware attacks. “Take these examples of ransomware attacks as a template to run a desktop exercise … to identify and determine how well your organization could cope in a similar situation,” said Brian Honan, founder and head of IRISSCERT, Ireland’s first CERT.

These cities won’t know the full scope of lost data until recovery efforts are complete. Lost data will include not only files not backed up, but also, transactions that cannot be rolled forward or recreated. “Beyond reviewing your IT assets to ensure appropriate backups are in place regularly, also document and revalidate areas where the risk of data loss has been accepted,” said Lee Neely, a Senior Cyber Analyst at Lawrence Livermore National Laboratory.

The term ransomware has been around for decades, but most daily computer and Internet users are blissfully unaware of the term or its consequences. A global ransomware heist that impacted entire state hospital systems, international businesses, and countries as a whole on Friday, May 12 put the illegal activity in the spotlight, hopefully creating a higher level of awareness for the general public – and companies who may have felt they were immune from such attacks.

Ransomware is modern day technology kidnapping. A virus infiltrates a computer device, locks down its data, and won’t release it until a ransom is paid – whatever that may be. On May 12, that ransomware technique was released via [“WannyCry,” a virus that was accessed via link](https://www.enterprisemobilityexchange.com/eme-security/articles/%E2%80%98wannacry%E2%80%99-ransomware-attack-impacts-70-countries). Once the user opened the link, the bug then encrypted that computer’s data and held it for ransom.

The virus was able to spread through large networks without user interaction thanks to a vulnerability in the Microsoft Windows operating system. Microsoft released a patch for the vulnerability, but the fix is only as useful as the user makes it – meaning it needs to be installed and run on each device.

This is where enterprises large and small are impacted - FedEx, Telefonica, and the UK's National Health Service on Friday - as a single user accessing the link or attachment essentially allows the bug to infiltrate the system as a whole if the system was vulnerable.

So, how can employees in your enterprise protect their individual devices from falling prey to ransomware attacks? Here’s a checklist everyone should be aware of:

* Always keep security software up to date on devices
* Keep the OS and other software updated by installing patches, which are created to secure vulnerabilities
* The most heavily used form of infection method is via email. Do not blindly open email attachments or links, especially if it’s not coming from a trusted source
* Back up important data. If an employee’s device was victimized by WannaCry, the encryption would not have had as severe an effect if that device’s data was resting elsewhere and easily accessible to the user

According to [The Verge](http://www.theverge.com/), within 48 hours of the virus spreading, it had reached more than 10,000 organizations and 200,000 individuals in more than 150 countries.

So how did this attack slow down? A single cyber security expert, just 22 years old, who goes by the name of [MalwareTech](https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html" \t "_blank) woke up Friday and went through his normal day-to-day motions, but noticed something was awry.

MalwareTech was actually off from work Friday and on vacation. In the blog post published Saturday, titled, “How to Accidentally Stop a Global Cyber Attack,” the unsuspecting hero says he woke up around 10 a.m. and checked into a UK cyber threat sharing platform, then headed to lunch with a friend. Around 2:30 p.m. he returned home, logged into the same platform, and said the thread was “flooded with posts about various NHS systems all across the country being hit, which tipped me of (sic) to the fact this was something big.”

The blog goes on to detail how MalwareTech found a previously unregistered domain name within the ransomware file, and was able to “sinkhole” the issue. Read more about how the [ransomware attack was slowed here](https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html).

While this threat was slowed within the first 24 hours, MalwareTech does believe a second version of the ransomware is on the horizon, and tweeted on Sunday:

*Warning for Monday: If you turn on a system without the MS17-010 patch and TCP port 445 open, your system can be ransomwared.*

Among the first organizations to be hit, the National Health Service, which provides healthcare for UK citizens, computers were locked up and encrypted Friday countrywide, forcing doctor’s appointments to be canceled or postponed and cancer treatments to be delayed, among other issues.