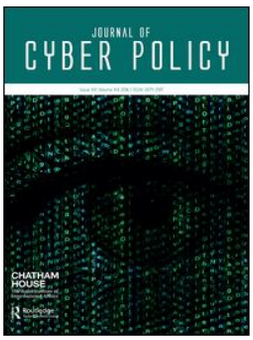

Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Cyber negotiation: a cyber risk management approach to defend urban critical infrastructure from cyberattacks

Gregory Falco, Alicia Noriega & Lawrence Susskind

To cite this article: Gregory Falco, Alicia Noriega & Lawrence Susskind (2019): Cyber negotiation: a cyber risk management approach to defend urban critical infrastructure from cyberattacks, Journal of Cyber Policy, DOI: 10.1080/23738871.2019.1586969

To link to this article: https://doi.org/10.1080/23738871.2019.1586969

Published online: 01 Mar 2019.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2019.1586969

Routledge
Taylor & Francis Group

Cyber negotiation: a cyber risk management approach to defend urban critical infrastructure from cyberattacks

Gregory Falco [a,b], Alicia Noriega[b] and Lawrence Susskind[b]

[a]Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA, USA; [b]Department of Urban Studies and Planning, Massachusetts Institute of Technology, Cambridge, MA, USA

ABSTRACT

Technical tools dominate the cyber risk management market. Social cybersecurity tools are severely underutilised in helping organisations defend themselves against cyberattacks. We investigate a class of non-technical risk mitigation strategies and tools that might be particularly effective in managing and mitigating the effects of certain cyberattacks. We call these social-science-grounded methods Defensive Social Engineering (DSE) tools. Through interviews with urban critical infrastructure operators and cross-case analysis, we devise a pre, mid and post cyber negotiation framework that could help organisations manage their cyber risks and bolster organisational cyber resilience, especially in the case of ransomware attacks. The cyber negotiation framework is grounded in both negotiation theory and practice. We apply our ideas, ex post, to past ransomware attacks that have wreaked havoc on urban critical infrastructure. By evaluating how to use negotiation strategies effectively (even if no negotiations ever take place), we hope to show how non-technical DSE tools can give defenders some leverage as they engage with cyber adversaries who often have little to lose.

ARTICLE HISTORY
Received 12 August 2018
Revised 10 December 2018
Accepted 17 December 2018

KEYWORDS
Negotiation; cyber risk management; ransomware; critical infrastructure; cyber resilience

Introduction

Cybersecurity is often portrayed as a 'cat and mouse' game that tests each side's relative technical prowess; however, it can also be considered a battle of social wits. Humans are behind every hack, and attackers have human motivations. The social science that ought to inform every effort to deter and engage attackers can easily be overlooked when cybersecurity experts focus exclusively on technical exploits and ways to counter them. We call the social science tools and techniques available to defenders, 'Defensive Social Engineering'. Some DSE tools include using honeypots as decoys (Cohen 2006, 646), announcing retribution for would-be attackers, also referred to as 'hack back' (Jayaswal, Yurcik, and Doss 2002, 380), and raising cybersecurity awareness through training. For this study, we focus on another underutilised social science strategy: negotiation.

In this paper, we propose applying negotiation practices to cyber defence in order to improve cyber risk management. We define cyber negotiation as a three-part process in

CONTACT Gregory Falco gfalco@mit.edu

which a defender prepares for, conducts and reflects on a digital interaction with an anonymous cyberattacker. Cyber negotiation does not require paying a ransom, nor should it be used in all ransomware situations. Rather, we focus on preparing for cyber negotiation as a risk-management strategy in ransomware attacks against urban critical infrastructure.

While many cyberattacks leave defenders with no idea about the attacker they are dealing with or their whereabouts, ransomware attacks are different. Ransomware generally involves solicitation of a payment in return for the release of data that have been stolen or the restoration of services that have been rendered inoperable. Some ransomware attackers even provide a channel of communication for the defender to connect via untraceable means. While this is not always the case, an invitation to communicate with a hacker provides an opportunity to directly engage in an exchange.

Urban critical infrastructure and services, including electricity grids, water networks, transportation systems and emergency services including police departments are all vulnerable to attack because they are digitised with 'smart' sensors and control systems connected to the internet (Assante and Bochman 2017). Smart city infrastructure is a prime target for cyberattackers considering their guardians' (public administrators) poor understanding of cyber risk, their vast surface area of attack, the value of their data and their societal importance (Falco et al. 2018, 48360–48373). For example, 123 of 187 closed circuit televisions (CCTVs) were compromised across Washington DC prior to the 2017 presidential inauguration (Williams 2017). The ransomware attack that disabled these CCTVs affected the police departments and the president's security detail from overseeing potential threats while their systems were down.

Even more recently, the US city of Atlanta sustained a ransomware attack on 22 March 2018. The ransomware locked down city computers and their associated services for many city functions and demanded approximately $51,000 delivered in bitcoin to return access (Greenemeier 2018). Affected services ranged from payment-acceptance for fines or fees to the processing of various online requests. The city jail had to revert to using pen and paper for operations (McCallister 2018). The city did not pay the ransom and this resulted in some services being offline for over two weeks. As of 5 May 2018, the total cost to recover from the attack has surpassed $5 million (Atlanta Department of Procurement 2018).

To test our ideas about the benefits of preparing for cyber negotiation (whether they exchange anything or not), we conducted an extensive search and evaluation of past ransomware attacks. We paid close attention to instances in which negotiation ensued, or in which there were missed opportunities for cyber negotiation that could have helped mitigate the damage caused by the ransomware attack. We also asked critical infrastructure and services operators to help us understand the cyberattack defences they have in place by participating in simulated ransomware attacks. The intent of these interviews was to understand how cyber specialists in a range of urban critical infrastructure agencies actually implement their cyber defence schemes. We analysed their responses through the lens of the three-step negotiation process we believe can reduce the risks and costs associated with malware attacks on critical urban infrastructure. We then assessed how our proposed cyber negotiation strategy might have helped in two well-known ransomware attacks on urban critical infrastructure.

Background

The nature of ransomware

Ransomware is a type of malware that takes a cyber asset hostage (Mansfield-Devine 2016, 8–17). A cyber asset has been taken hostage when it has been made unusable by an attacker but use may be returned after the attacker's demands have been met. From an IT perspective, this usually involves encrypting an organiation's data. Once data are encrypted, a key is required to decrypt the files and enable access once again.

Sometimes the data are not encrypted but actually destroyed or exfiltrated by an attacker (Carbon Black 2017). Hackers make money by charging a fee for the key to decrypt the files they have secretly encrypted.

Ransomware only recently became a major threat, in part because of the emergence of bitcoin, a pseudo-anonymous payment mechanism, and Tor, a tool used to anonymize internet activity. Together, bitcoin and Tor provide a means for attackers to extract and transfer ransom payments while maintaining their anonymity. Prior to bitcoin and Tor, it was relatively easy to track down a hacker by following a ransom payment back to them. This new untraceable payment scheme, along with 'ransomware-as-a-service' kits make ransomware a profitable and simple attack mechanism. Ransomware kits are sold on various darkweb/black market sites by criminals, terrorist organisations and even nation states. While there are many different kits available, they are all intended to make launching a ransomware attack 'plug and play.' There are even sophisticated economic models set up by would-be criminals to help fund and distribute ransomware (Carbon Black 2017).

The simplest method of blunting the effects of a ransomware attack is to be certain that all of an organisation's data are continuously backed up and stored on a separate network or in a location that is remote and entirely disconnected or air-gapped. While it may seem obvious that organisations should back-up their systems on a regular basis, almost 63 per cent of organisations do not (Klein 2017). While many IT systems will not suffer substantially when a transition is made to a back-up system, most urban infrastructure is classified as Operational Technology (OT), not IT. OT involves cyber-physical systems (i.e. digital devices that impact the physical world), which generally cannot be taken offline while transitioning to a back-up system without causing a substantial impact on operations. Taking OT offline can result in severe consequences such as power outages or sewage leaks. If ransomware infects even a small part of an urban infrastructure network, the whole system may have to be taken offline to install a back-up. This could have profound physical and financial implications (Krebs 2016). So while backing up systems is, in theory, a good way to forestall the adverse effects of ransomware attacks, urban critical infrastructure systems have special features that make this less than an ideal strategy. NIST's guidance on disaster recovery for OT acknowledges this challenge and proposes the need for running a parallel system (Stouffer, Falco, and Scarfone 2011).

An example of how long it can take to restore an urban critical infrastructure system is offered by a ransomware attack against a major transportation authority which took place in 2016 (Rodriguez 2016). The transportation authority was able to maintain system operations during the attack by resorting to handwritten bus route assignments, but it chose to take down fare-payment systems from Friday, 25 November to Sunday, 27 November

while restoring its software. This resulted in revenue losses of about $50,000 (Rodriguez 2016). While the transportation authority refused to pay the 100 bitcoin ($73,000) demanded by the hacker, many businesses that are ransomwared do pay. According to a 2016 IBM study, 70 per cent of executives from (private) companies who have been ransomwared paid the hacker (IBM 2016).

In the case of ransomware attacks against urban infrastructure, it is not always easy to gauge the health of a cyber asset that has been or is being held hostage. This is largely because the defender has no way to determine what is happening to their data while it is inaccessible to them (it could be posted or sold on the dark web). While data are potentially recoverable once a decryption key is provided by the attacker (after the ransom has been paid), an asset could be permanently compromised from a reputational and competitive advantage standpoint even if the data are returned intact. Thus, damage caused by a cyberattack can extend well beyond the immediate damage caused by system downtime.

After an attacker targets a system and encrypts the data such that the asset is compromised, the operator usually has the option of paying a ransom or restoring functionality by deploying a back-up system. There is no reason to believe, however, that the hacker won't be back. A recent ransomware trend indicates that once a ransom is paid, attackers lie dormant in the system they hacked and reappear, instigating the same kind of attack again (Carbon Black 2017). There is no simple way to know if a hacker still has access to a system after an attack. This is why many organisations choose to re-flash the firmware of their devices after an attack and rebuild. This was the case in the CCTV hack in Washington DC (Williams 2017).

Applying negotiation theory to cyber risk management

There are three stages in a digital, anonymous negotiation: pre-interaction (setting expectations, arranging the situational context and preparing organisationally), during interaction (whether face-to-face or not) and after interaction (post-assessment and lesson-learning for organisational improvement) (Köszegi, Kersten, and Vetschera 2002, 418–427). Contrary to popular perceptions, most of a negotiation happens before or after the actual attack interaction itself. We aim to contextualise and apply this three-part understanding of negotiation to how urban critical infrastructure operators manage the risk of being attacked by ransomware. In doing so, we consider leading theory in hostage and ransom negotiations, described below.

Bans on ransom negotiation

US federal statutes bar the payment of maritime piracy ransoms (Lennox-Gentle 2010, 199). Should the official US stance on non-payment of maritime pirates apply to ransomware attacks as well? The basis of the ban rests on the theory that paying ransom encourages repeat and copycat behaviour. According to the World Bank, as much as 20 per cent of ransom proceeds are put aside to fund future attacks (Dutton and Bellish 2014, 299). Despite investing in deterrence such as navy escort patrols, rerouting shipping routes and faster steam engines, pirate attacks continue.

The US and UK governments decided that the best way to deter would-be pirates from choosing piracy as a career 'and thereby protecting seafarers from continued threat of

hijackings and hostage-takings' was to eliminate ransom payments. Of course, banning ransom payments to hostage-takers may have put innocent lives at risk. While banning piracy ransoms may be good for the world community, it only works if everyone participates. Thus, the policy raises a collective action problem. Some states or individuals may prefer to pay ransom in the short-term. If they do, they undermine the effectiveness of the policy for everyone else (Dutton and Bellish 2014, 299).

Human hostage vs digital hostage

There is substantial literature concerning hostage negotiation. The goal is for the hostage negotiators to position themselves as deal brokers and identify mutual interests with the hostage-taker (Vecchi, Van Hasselt, and Romano 2005). Ransom negotiation almost always involves moving through a communication stage and developing rapport with the attacker, buying time, defusing intense emotions and gathering intelligence to ascertain the optimal negotiation or intervention strategy (Lanceley 2003). The Behavior Change Stairway Model (BCSM) developed by the FBI's Crisis Negotiation Unit explains how this kind of relationship-building works (Vecchi, Van Hasselt, and Romano 2005, 533–551).

While many of the ideas from human hostage negotiation can inform negotiation in ransomware situations, most of the tactics involved assume human contact between the hostage-taker and the victim and/or between the hostage-taker and the negotiator. It is this contact that is used to generate empathy that skilled negotiators use to build trust. It turns out that empathy and trust have also been established in some ransomware 'experiments' done by a team at F-Secure. They posed as a ransomware victim and got attacker-agents to extend payment deadlines, lower ransoms (three out of four crypto-ransomware gangs negotiated, leading to a 29 per cent average discount), and provide step-by-step assistance regarding how to pay in bitcoin after feigning ignorance (F-Secure 2016). The hacker who targeted the previously mentioned transportation authority was himself hacked shortly after his ransomware attack against the transportation authority (Krebs 2016). The hacked emails of the attacker revealed that other victims besides the transportation authority had successfully negotiated down their ransom payments. Another victim, China Construction of America Inc. was ransomed for 40 bitcoin, but ended up negotiating a payment of only 24 bitcoin (Krebs 2016).

Research plan and interview protocol

To understand how urban critical infrastructure operators are likely to handle a ransomware attack, we developed a hypothetical ransomware scenario and simulated an attack (with permission) using screen captures from past attacks. Before initiating the simulation, we asked the operators some questions about their organisation's cybersecurity posture.

Our pre-simulation questions included:

(1) Do you have a cyberattack response plan in place for your system?
(2) What, if any, technologies do you use to fend off hackers?
(3) What, if any, non-technical strategies do you use to fend off hackers?

These questions set a baseline for our assessment of the urban critical infrastructure manager's preparedness. To begin the scenario, we showed the operators an image of

a port scan detected on an intrusion detection system. This was followed by a series of questions aimed at ascertaining how the operators would respond if they actually saw such images. Next, we showed a ransomware screen indicating that files had been locked and that a payment in bitcoin was required to unlock them. At this point, we asked how the operator would respond, and whether (and how) they would engage the hacker to explore the possibility of negotiation. Finally, we showed the operator a screen indicating that the attack had been resolved. This was followed with questions about how the urban infrastructure organisation might incorporate lessons from this hypothetical attack into their future cybersecurity efforts and whether damage control might be managed differently in the future. Our simulation screens and associated questions are included in Appendix A.

Finding critical urban operators willing to participate was difficult. Some declined because they did not want to draw attention to themselves or their organisation. Others appeared not to have a cybersecurity strategy in place, and did want that to become obvious. Some were unable to get permission from their leadership to speak with us about cybersecurity strategy (although highly sensitive information was not requested). We approached 100 organisations by email. The solicited organisations were selected because they were either a) previously in the media because they had experienced a ransomware attack or b) within close geographic proximity of members of our research team in Massachusetts and California. This gave us an opportunity to conduct our interviews in person. Ultimately, of the 100 organisations we approached, seven agreed to be interviewed. We are not disclosing their names. They participated because we promised to preserve their anonymity. We are allowed to say that they represent police departments, electricity utilities, government agencies, satellite operators (weather and GPS), emergency management services and transportation departments and were from the states of California, Connecticut, Massachusetts and Vermont. All interviewees answered questions individually, although in one instance three organisations met together to participate in the simulation. We asked that everyone who participated respond to our questions individually in writing so we could be sure they were not influenced by the other respondents. Each interview took approximately thirty minutes to complete. Interviews were audio recorded for our review, and the recordings were later destroyed. We also took written notes during each session. The individuals we interviewed held positions such as Chief Executive Officer (CEO), Chief Information Officer (CIO) and Chief Information Security Officer (CISO). Everyone we talked to had an opportunity to review our study results and correct any misinterpretations of their inputs. Our research design was approved by MIT's Committee on the Use of Humans as Experimental Subjects.

Because of the small number of interviews, we augmented this research method with cross-case analysis of actual urban critical infrastructure ransomware attacks reported in the media. The two cases include an attack against Uber and the WannaCry ransomware attack. We fully acknowledge that the small number of interviewees is a limitation of our study. The findings and insights of this research may not be applicable to all urban critical infrastructure organisations, but we believe it is a strong starting point for understanding how using a negotiation framework (even if actual negotiations never take place) can help operators to prepare for, defend and recover from attacks.

Interview insights

To generate our cyber negotiation-oriented risk management strategy, we analysed our interview findings and the results of our cross-case analyses during three time periods: pre-attack, mid-attack and post-attack. As you will see, the urban critical infrastructure operators we interviewed did not focus very much on the actual mid-attack phase. They spent considerably more time describing how they would prepare for a cyberattack and how they would respond after one occurred. The pre-negotiation, mid-negotiation and post-negotiation framework seemed very comfortable for the infrastructure managers with whom we spoke.

Pre-attack cyber negotiation

Pre-cyberattack negotiation seems to be focused mostly on getting clarity, if not agreement on the assignment of responsibility and lines of authority. To properly prepare an organisation for the possibility of a cyberattack (and possible negotiations), we learned it is crucial to develop a cyber incident response plan, build organisational awareness of the plan and the potential for attack, deploy the proper technology to defend systems, formalise the internal and external lines of communication that will be activated during an attack, and establish relationships with selected external organisations (especially the FBI). This pre-attack phase of cyber negotiation is aimed at establishing points of internal leverage to use during an attack and subsequent negotiations. Without adequate leverage (e.g. authority) developed during this phase, few if any negotiation options are likely to emerge. We briefly discuss each pre-attack component (and the negotiation leverage involved). Again, those suffering a breach may not be willing to pay a ransom, but that doesn't mean that they should not seek to interact with their attackers. As you will see below, there are strategic advantages to be gained by engaging in negotiation even if no deal is reached.

Develop a cyber incident response plan

From our interviews we gathered that many critical infrastructure and service organisations already have general incident response plans. The CISO of a utility said, 'These [incident response plans] are the first line of defence in case of cyberattack'. While potentially useful in ransomware situations, they are not specific to cyberattacks and are aimed at any kind of 'incident' that might occur. At present, incident response plans are the go-to guide for critical infrastructure operators if they are under attack. A CIO we interviewed commented that 'Most incident response plans do not offer detailed instructions; instead, they recommend turning to outside resources such as the FBI and Homeland Security for assistance. […] They instruct managers under attack to convene a pre-named management team of internal authorities relevant to the incident type to make operational decisions in real time'. The actual response to each event varies considerably (based on our interview findings). Organisations typically look to their CIO for guidance on how to deal with specific incidents and whether (and when) to consult their ISP or the FBI, depending on the severity of the event. It appears that the CIO has decision-making power over what happens during an incident. A CIO from a state agency we interviewed commented that '[Our] ransomware-specific incident response plan was rather simple – wipe the system and restore from back-ups'.

While this might work in some ransomware scenarios, it might not be feasible in all situations. For example, some organisations do not make back-ups in real time. This means that critical data could be missing from the back-ups when it comes time to restore the system. Such cases make more difficult the decision to 'wipe the system and restore from back-ups,' as some data might be lost. Therefore, incidents will have to be evaluated on a case-by-case basis. We learned that some incident response plans, depending on the organisation's sophistication and its CIO's knowledge of cyber response, may include only the bureaucratic documentation needed for disclosure purposes and the reduction of legal liability, instead of a robust guide to how best to respond to specific cyber incidents.

Incident response plans are widely available on the internet for organisations to adapt to their needs. One of the CIOs we spoke to said that 'It is the responsibility of the CIO to manage and maintain these plans on an annual basis'. A popular reference resource is the University of California Berkeley's Incident Response Planning Guidelines (Berkeley 2018).

Build awareness

All the critical infrastructure operators with whom we spoke indicated that they had some mandated employee training and awareness campaigns regarding cybersecurity in place.

However, some organisations take this more seriously than others. A utility CEO commented, 'Building awareness is not sufficient'. Instead, he tries to foster a 'culture of security'. He aims to 'instill cybersecurity thinking across all aspects of his organization's employee experience'. This involved aligning employee priorities and success metrics with cybersecurity best practices. An example would be to report the number of successful phishing attacks against an employee as part of their annual job performance review. Also, he insisted that 'Leadership must support a cybersecurity culture by not only encouraging it, but outwardly practising good cybersecurity'.

In contrast to this utility CEO, we spoke with a CISO who mentioned that their

> cybersecurity awareness programme consisted of a computer-based training programme that is required when employees complete their annual HR training. The training is 30 min long and was created by an outside consultant. It explains what a phishing attack is, and encourages employees not to leave their laptops unlocked. There is a test at the end which employees must pass to complete the training.

Upon pressing further, we learned that employees can take the test as many times as they want and there is little accountability for knowing the material after the course is over. The CISO said 'Cybersecurity training is seen more as a compliance exercise than as an actual educational tool'.

Despite the varied approaches, four of our seven interviewees acknowledged the importance of building awareness in advance of possible cyber incidents because employees are the first responders in any attack. The state CIO stressed that 'When an employee notices a ransomware attack or some other unusual cyber activity, they should immediately communicate the incident. A quick response can help limit damage to the defending organization since ransomware attacks have countdown timers'. Often, hackers threaten to inflict increasing damage to the system if action is not taken by the deadline.

Deploy technical defences

The cyber negotiation framework should be used in tandem with technical defence strategies. All seven of our interviewees described the myriad technical defences used by their organisations. Importantly, the CISO of a transportation agency said, 'Technical defences can detect an intrusion on a network, but cannot resolve the problem – especially when a ransomware attack is underway'. Such tools should provide insight into the attacker's identity such as their IP address or the various attack vectors they used to penetrate the network. This is important background knowledge that can be used during the attack post-mortem. It might also provide some insight into the motives of the attackers. The CISO of a major satellite operator said, 'A system manager can never have enough information about a potential cyber negotiation adversary – especially when so much of the interaction is cloaked behind layers of anonymity'. This is one reason that four out of seven of our interviewees' organisations spend millions of dollars a year to keep up with some of the subscriptions they rely on to enhance their technical security. Some popular technical security subscriptions named consistently by five of the seven interviewees included Palo Alto Networks which focus on intrusion detection and network security (Palo Alto Networks 2018), Mozy (2018) which provides back-up services, and McAfee (2018) which provides endpoint antivirus protection. The transportation CISO said, 'Backing up systems is critical to preparing for the possibility of cyberattack and subsequent negotiation'. Having a back-up system is, in fact, a source of substantial leverage in a cyberattack negotiation. One may think that there is no need to negotiate if an urban infrastructure operator has a back-up, but this is not the case. The utility CISO we spoke with said,

> Installing back-ups requires taking a system offline and rebooting it. Because of the 24/7 operational nature of urban critical infrastructure systems, it might be better to negotiate return of system control than taking the system down to transfer to the back-up. Also, switching to the back-up and cutting off communication with an attacker means that an organization might be vulnerable to another attack of the same kind.

It might also mean that an organisation has lost control of important confidential information. Thus, it would be better to get all that information back, even if that requires paying a ransom.

Formalise communication channels

The emergency services lead we spoke with from a US state agency said,

> It is essential to have clear and formal communication pathways in the event of a cyberattack. […] Because a wide range of employees interact with computing systems that can remotely communicate with urban critical infrastructure, each one must know who to contact (and in what order) if they are the victims of ransomware.

When speaking with the CIO of an urban transportation authority we learned that their network is directly connected to other urban infrastructure networks in the state. This is not uncommon. Networks are designed in this fashion to enhance ease of access for maintenance and third-party service providers. She said, 'This can result in a civil servant unintentionally infecting a system despite having no direct interaction with it'. Therefore, every employee must know who to contact if there a breach, and what information they will be

asked to provide. While upward and downward internal communication plans are crucial, external plans need to be established as well. The utility CEO told us that

> Cyberattacks often attract considerable media attention. If information about organizational chaos is leaked during an attack – as opposed to a clear and calm message about how the attack is being handled, we will be at a severe disadvantage during any cyber negotiations.

A CEO we interviewed described a very strict external communication protocol their organisation intends to follow during a breach.

> The script for each dialogue will be created in real time by the CIO or CISO and then shared with the organization's legal team. General Counsel tends to take a heavy-handed approach to restructuring such communications. The public relations team is then supposed to approve the message for external use. Either the CEO or CIO is responsible for communicating the message to the press. The information that is ultimately conveyed is highly sanitized and likely to say very little about the actual incident.

We learned that information about what actually happened is often leaked to various media outlets by employees after the press briefing. The external communication process described by our interviewee sounded extremely cumbersome. We are not sure what will actually happen under pressure. Two of our interviewees including the CIO of the state agency did 'not know if an external communication protocol was in place' for their organisation. He said, 'We would just contact the public relations team'.

Establish external organisational relationships

All seven urban critical infrastructure operators we interviewed indicated that they would be quick to call in external help if they were targeted by a ransomware attack. The utility CEO said, 'It is extremely important to build a relationship with the authorities and the FBI before we have to deal with ransomware'. Others mentioned their relationships with national labs that do attack aftermath evaluations. Our utility interviewees indicated that Idaho National Labs has established a team to help with post-mortems for cyberattacks on industrial control systems. The transportation agency CIO said, 'We have relationships with consultants who specialize in attack forensics and cyber negotiation' who help manage attack issues. We learned that prior to a first cyberattack or cyber negotiation, some urban infrastructure operators establish relationships with private entities who can assist in case of attack. When an attack is underway, however, is not the time to try to sort out lines of responsibility with private contractors.

In summary, most of our respondents have made contact with the FBI and have an open line of communication to them in the event of a breach. However, five of the seven interviewees did not have a clear understanding of what they would do and what the FBI would do during and after an attack. Some indicated they would 'turn over operations' during an incident to an external consultant who would make decisions for them in conjunction with the FBI. Others thought that the FBI would assist as their own internal organisation managed the attack. Six of the seven interviewees agreed that their own organisation is ultimately responsible for deciding when and how to resume operations.

The attack

During an attack, an urban infrastructure organisation must act quickly; hence the pre-attack negotiation preparation measures identified above. Insights about the prospect of engaging in cyber negotiations varied across our interviewees. Some strongly opposed the idea of negotiating an exchange with a hacker, saying 'We are morally opposed to giving anything to criminals'. Some were open to negotiating 'if a capable party [i.e. someone other than themselves] were going to lead the effort', although they simultaneously wanted to retain final decision-making authority. Others indicated an interest in cyber negotiations as a technique for buying time. A memorable point made by one utility executive is 'Urban critical infrastructure operators should never say never to negotiating'. It turns out there are a variety of objectives that can be met through negotiation, even if the victim has no intention of paying a ransom. Gathering more information about the attacker so they might be identified and brought to justice, for instance, may be a worthwhile objective of negotiation. While not all operators agreed that negotiating is the right thing to do, all had ideas about how a cyber negotiation would probably unfold. They envisioned the following steps: convene the incident command structure, evaluate the severity of the event, consult the legal team and bring in and brief outside experts to execute the negotiation. Each of these steps is described below based on our interviewees' feedback.

Convene the incident command structure

As part of the incident response plan, each urban critical infrastructure organisation described a team of internal stakeholders and leaders they would convene in the case of a cyberattack. The utility CISO commented that 'The incident command structure must decide how to proceed so that responsibility does not fall on the shoulders of one (unprepared) individual'. The group is not responsible for problem-solving during the incident, however; they are the chief decision-makers. For example, this group might ultimately decide that a ransom should be paid. They would also be responsible for decisions such as when to call in the FBI and report the incident externally. For private companies, such groups function autonomously. We learned that government-affiliated organisations, however, are unable 'to refer an incident to a command structure during such cases. Instead, we need to wait for guidance from our governing body before responding to a ransomware incident'. This means that they are not able to act until explicit instructions come from the most senior level of the agency.

Determine event severity

After the incident command structure is assembled, the team needs to evaluate the severity of the attack. Often, the incident command structure team cannot do this on their own, so they consult operators closest to the system in jeopardy. 'Severity is determined by the number and criticality of the systems impacted,' said the CISO of a utility. Criticality appears to be judged largely on the amount of downtime the infrastructure system can withstand. If a system is not determined to be highly critical, three of our interviewees informed us, the 'infected' system might be taken offline and rebooted using back-ups. 'If a system is deemed critical, and cannot be taken offline even for a short period without serious consequences like the potential loss of life caused by turning off power

during a freezing night, negotiations might then begin,' according to the utility executive. In a ransomware incident at one CIO's transportation agency, 'Instead of paying a ransom, we chose to shut all payment systems down. This literally opened the gates of the rapid transit system, allowing customers to pass through fare-free as we tried to install a back-up and reboot'. Smaller groups, such as the precinct of a police chief we interviewed 'do not have complete back-ups, cyber incident response teams or alternate recovery options. So when we were hit with a ransomware attack, our IT department advised that we pay the ransom'. Our interviewee's incident is not inconsistent with other news stories in which police departments have paid ransoms. One public report describes how ransomware infected a department's TriTech software responsible for dispatch and police records. Without this, they would have been unable to operate. That was not an option (CNN 2016). This might have been a good opportunity for cyber negotiation, but that was not tried.

Another interviewee whose agency had experienced a ransomware attack commented, 'We had to determine the severity of the risk to our system at the time of the incident. Rather than paying the ransom, we determined that the risk was limited to our financial systems and would not impact operations'. The financial system was shut down until back-ups could be restored. In this interviewee's case, because the ransomware was isolated in the financial system, the risk calculation was based on financial losses as opposed to a potential operational disruption which would involve public safety, negative publicity and political factors in the risk calculation. There are no standards agreed upon for calculating cyber risk. This is one reason why the cyber insurance business is still struggling to find adequate underwriting (Orcutt 2017). Following on from our own research, we are hoping to work with the insurance industry to develop a research agenda to improve the viability of cyber insurance as a strategy to manage cyber risk.

Consult the legal team

According to two of our interviewees, and summarised by the emergency services lead, 'Before any purposeful action can be taken, the General Counsel or several internal and external legal advisers need to be consulted'. It is their job to calculate the organisation's liability under various scenarios. Lawyers specialising in cyber risk are asked to provide guidance on the organisation's options. Often, the General Counsel is a member of the incident command structure, but all seven of our interviewees made it clear that consideration of legal liability is a distinct step. The utility CISO said, 'In addition to briefing the incident command structure on potential liability, the legal team must advise on any cyber insurance coverage the organization might have, and whether it is appropriate to engage the insurer'. Legal specialists are extremely important in decision-making about cyber negotiation, especially in publicly-owned organisations which in the US have local, state and federal obligations regarding hack disclosure. Whether it is with legal or other advisers, infrastructure managers who are the victim of an attack need to figure out quickly what their approach to negotiation will be. They could negotiate just to gain enough time to switch to their back-up systems. Or they could enter into negotiations to see if they can reduce the ransom request, delay the timing for its payment or avoid it all together. They could negotiate with the FBI in a way designed to get more information about the hacker. Negotiation doesn't assume that a ransom will be paid.

Negotiate

None of the interviewees had much confidence in their own organisation's ability to proceed with a cyber negotiation in real time. Everyone we interviewed assumed that negotiation experts would have to be called in. State agencies we spoke with indicated that the FBI would be called immediately. Private sector urban critical infrastructure operators also indicated that they would depend on the FBI, in addition to calling on help from private cybersecurity contractors specialising in ransom attacks and cyber negotiation. A comment from the lead of a US state emergency management service was that 'When the FBI is contacted for a cyber security event involving a public agency, they will immediately assume control of all systems. The infrastructure operator will no longer have any say about operations'. Upon speaking with the FBI cybercrime division in Boston, we learned that this is not the case. This disparity points to the larger issue of the inaccurate expectations of infrastructure operators. The FBI said, 'Our role is conducting forensic analysis and trying to catch the hacker'. This is one reason why it might be advisable for urban infrastructure organisations to call in a private contractor in addition to the FBI so that the private contractor can help with incident response and system recovery. The FBI's official stance is that they will not negotiate with cyberattackers (and that urban critical infrastructure operators should not either). This raises the utility CEO's comment mentioned earlier – never say never. In such critical moments, all options ought to be on the table.

Post-attack

When an attack is over, almost every cyber negotiation continues, although not with the attackers. All seven of our urban critical infrastructure operator interviewees revealed that whatever pre-attack measures they had put in place needed to be re-evaluated in light of what happened (or what has happened to others). Additionally, five of our interviewees identified other post-attack considerations, including putting in place a required post-mortem attack report, documenting and implementing whatever lessons were learned and initiating external damage control. Some organisations take post-attack negotiation steps more seriously than others. For one of our CISO interviewees, 'Our ransomware attack motivated a full review of all our systems and security'. The attack prompted them to launch security awareness training for all new employees. Post-incident, their information security team prepared a review and recommended that 'we have stricter password update policies and rework our firewall configurations'. Post-attack negotiations in the public infrastructure arena often include allocating blame and constructing a narrative for public consumption about what happened and why. Instead, the goal should be to reduce the risk of further attacks and restructure organisational dynamics that create vulnerabilities.

Develop a post-mortem attack report

Extensively documenting and conducting a digital forensic investigation of an attack (i.e. the steps leading to the attack, the attack vector exploited, the response protocol followed) was noted by several operators as an essential preparation for subsequent attacks. 'Without documenting what happened, there is no way to identify opportunities for improvement,' said the satellite operator CISO. A post-mortem can elucidate missed

opportunities for gaining leverage in subsequent negotiations. Six of the seven interviewees agreed that a review is critical following an incident; however, two of the seven admitted they did not have time to do this following the breaches they had experienced. This was not surprising because their priority was restoring operations. Once they were restored, all focus returned to day-to-day management.

After-event review is de-prioritized once the frenzy of an attack is over.

Share information

While reconsidering what happened is very useful to an organisation, five out of our seven interviewees described their desire to know more about what happened to other victims of cyberattack in their industry. Unfortunately, every victim's priority is to protect confidential information, making it hard to aggregate information on attack patterns. At present there are no US federal or state mandatory reporting requirements. The utility CEO we interviewed underscored the importance of information-sharing. He commented,

> If a post-mortem takes place and stories are shared with the broader security community, feedback on how the attack was handled could be analysed by both internal and external experts. Relationships can be built with external experts who will be in a better position to provide advice and assistance in the future.

Many critical infrastructure sectors such as utilities participate in Information Sharing Analysis Centers (ISACs). The US National Council of ISACs indicates that there are 24 such organisations developed expressly for the purpose of sharing threat and security information within industry sectors. The idea behind ISACs is that if one organisation is breached and notifies others, a vulnerability might be remediated before a hacker takes advantage of it elsewhere in the community. Our understanding from two interviewees is that some ISACs have a stronger participation of industry constituents than others. For example, the utility and financial ISACs have a very proactive membership base as opposed to the newly formed automotive ISAC.

Other external experts that could be called upon are organisations such as the previously mentioned Idaho National Labs (INL). INL offers a test bed for electric utilities to simulate attacks and defences. They also have a strong incident response team that can be flown in to help with post-mortems. They are called the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (INL 2018). CERTs exist all over the world to aid in cyberattack preparation and post-mortem analysis. Interestingly, only the utility CEO and CISO mentioned said they might call a CERT.

Document lessons learned

'Preparing a summary of lessons learned from each attack is essential,' according to the emergency services lead. The CIO of one US state agency expressed the need after an attack for a concrete action plan to incorporate lessons learned into existing programmes: 'Our lessons learned are incorporated to incident response reports and future plans'. Others indicated that lessons learned should not be theoretical. Instead, action implications should always be drawn. For example, a US state agency CIO we spoke with insisted that 'All lessons learned should be immediately addressed in a highly visible manner by the leadership of the organization'. He continued,

> If staff in a certain department consistently clicked on phishing scams, that department should be targeted for additional phishing training, and should either be called out for their failure to protect cyber assets or commended if their resilience level improves.

The CIO encouraged 'visible and transparent measures to fill vulnerable security holes' in the organisation. This could improve the organisation's future negotiation positioning because hackers may publicly see the efforts taken to ameliorate past issues and move on to a different target.

Conduct external reputational damage control

External damage control was among the most discussed topics in our interviews. All of the urban infrastructure organisations we spoke with expect considerable blowback in the case of a breach. Both public and private organisations know they have to find out what kinds of information may have been compromised or stolen and the criticality of that information. Decisions must also be made about the best way of handling communications and subsequent repair of reputational damage. 'Handling messaging post-attack is an extremely sensitive topic that only certain leaders are authorized to handle,' according to the CIO of the transportation agency. Messages must be carefully crafted. None of the interviewees wanted to draw attention to their organisation after an attack – even if their primary message is that they have since fortified their defences. This type of outward messaging was presumed to invite further hacking against their organisation. Finally, one transportation CIO we spoke with said that 'Public agencies need to work with auditors to establish that they acted in good faith and were doing all they could to protect the taxpayers' best interest during the breach'. Two of our interviewees noted that 'Properly handling reputational damage control could be a form of leverage against future attacks.' If a hacker's goal is to undermine an urban infrastructure organisation's reputation, but the reputation is well-managed after a breach, this might discourage a future hacker from pursuing the same organisation a second time.

Cross-case analysis

After interviewing and aggregating insights from our interviewees about their attitudes toward and experience with pre, mid and post cyber negotiation with attackers, we evaluated two publicly documented cyberattacks using the negotiation framework that emerged. By reviewing these cases after the fact, we will show how the failure to treat the attack interaction as an opportunity for cyber negotiation contributed to suboptimal outcomes for the victim organisations. In the first case, the attack was a ransom cyberattack (without ransomware) in which the company chose to engage in a negotiation exchange with the hackers (but neglected the pre- and post-negotiation work that would have protected them). The second case involves a widespread ransomware attack in which there were many missed opportunities to use a cyber negotiation framework before, during and after the attack.

Uber technologies

Modern transportation infrastructure in cities consists of mass transit in the form of buses and trains, personal vehicles and taxi services. Increasingly, the traditional model of hailing

a cab to catch a ride has disappeared in favour of calling a cab on a digital platform such as Uber. In 2017, Uber had between 1 and 2 million active drivers in the United States (Berry 2017). While Uber considers its drivers contractors rather than employees, it collects and retains considerable amounts of data about all of these contractors – past and present. Not only does Uber store data about its drivers, but also its users. Uber's co-founder and former CEO Travis Kalanick mentioned in 2017 that Uber had 40 million active users each month (Lynley 2017). This makes Uber a prime target for hackers seeking personally identifiable information about a diverse and large population (e.g. all present and past Uber users and drivers).

In 2016, Uber covered up a major data breach that exposed 57 million user accounts, including data from both drivers and users (Greenberg 2017). Most of the data stolen consisted of names, email addresses and phone numbers. Additionally, 600,000 US driver licence numbers were stolen (Newcomer 2017). This hack was achieved by two hackers who accessed a private Github account used by Uber engineers. They stole credentials embedded in code on the Github site from an Amazon Web Services account where the data was stored (Greenberg 2017). Interestingly, the hackers did not encrypt or lock down the information. Nor did they agree to release it if a fine were paid. It is unclear if this was impossible given the constraints on the hackers, or if it was just not the preferred negotiation strategy. Instead, the hackers contacted Uber via email requesting funds to keep the breach quiet and not to disclose the data (Newcomer 2017).

Details are not available about how the negotiation unfolded, but ultimately Uber paid $100,000 to meet the hackers' demands under the guise of their bug bounty programme (Newcomer 2017). Bug bounty programmes are generally meant to reward white-hat hackers to find vulnerabilities in a system – not to pay off hackers who threaten the organisation. What we do know is that the hackers kept their side of the bargain after being paid. The only way the public found out about the hack was when the newly installed CEO, Dara Khosrowshahi, announced the breach after learning of the incident. The 2016 breach was hidden from the US Federal Trade Commission (FTC) which, at the time, was investigating a separate data breach Uber experienced in 2014 (Newcomer 2017).

While we cannot fully ascertain the details of what happened, it is clear that cyber negotiation was used to resolve this exploit and defend the digital platform. As we determined through our interviews with urban critical infrastructure operators, there were three discreet phases of the negotiation – pre-negotiation, negotiation and post-negotiation. Our interpretation of how these phases unfolded during the Uber attack are outlined below.

Pre-attack

Based on publicly available information, our understanding is that there was no cyber incident response plan in place at Uber. If there was, it must have not been followed during this incident. Before the attack, it seems that Uber did not take appropriate precautionary measures to secure its credentials on the Github account. Further, formalised communication pathways for reporting the threat, either internally or externally, did not appear to be in place or followed. Finally, it seems that no external connection was pre-emptively established during or after the hack. Uber appeared to have put its energies into hiding the attack from investors, customers, drivers and the FTC. We assume that Uber had no help from the FBI or other cyber experts in pursuing the negotiations as they did.

The attack

During the attack, hackers were able to collect data that were vital to Uber's reputation. This was used as leverage in the request for a ransom payment. After the ransom was demanded, some form of an ad hoc incident command structure was assembled. We know that a deal was arranged by the CISO and agreed to by the CEO (Benner, Isaac, and Frenkel 2017). Because of the eventual payout to the hackers, we assume that the CISO and CEO calculated that the data breach was a severe event. We also assume that legal counsel was sought because the director of security and law enforcement was fired along with the CISO after the breach and the ransom payment were exposed. Further, the CISO was a trained lawyer who had practised law previously and studied cyberlaw at University of Miami (Benner, Isaac, and Frenkel 2017). To initiate the negotiation, the hackers contacted Uber directly via email. Because they did this, and did not use a third-party service to issue their ransom demand, we assume that the hackers were willing to engage in a conversation regarding their financial demands and what they would offer in return. The parties were able to arrive at a mutually agreed amount ($100,000).

Post-attack

After the attack, the hackers maintained their side of the deal as the 57 million users' and drivers' data were never released (at least not publicly). It is unclear if a post-mortem attack report was ever made beyond the financial documentation indicating the payment made to the hackers. Uber chose not to engage authorities, share information or notify users of the breach. This was a missed opportunity for raising awareness of whatever vulnerability exposed Uber to the attack in the first place. It also made Uber continuously vulnerable to similar attacks until the attack was disclosed broadly. Further, as far as we can tell, no lessons learned were documented or acted upon. We wonder what precautionary measures Uber took in case the hackers defaulted on their agreement and released the user data. Finally, no external reputational damage control was done at the time. This ended up causing even worse damage for the company when word was finally released. In part because of its poor post-attack handling of the breach and its failure to disclose what happened to users, Uber lost its licence to operate in London (Finkle and Somerville 2017). As of May 2018, there are financial repercussions for failing to disclose data breaches under the European Union's recently adopted General Data Protection Regulation (GDPR). If the failed disclosure had occurred after GDPR was instituted, Uber could have been subject to fines of up to 4 per cent of their annual revenues (Meyer 2017).[1]

National health services

Healthcare institutions ranging from urgent care centres to hospitals are essential to everyday life in our urban centres. Such urban critical infrastructure collects and retains sensitive data about patients. Not only is sensitive data stored by healthcare institutions, but constant access to these data are required in real time to prepare for and perform procedures and surgeries for patients. Typically, data are stored in electronic medical records (EMRs). Their paper equivalents have been discontinued in many healthcare systems. These data consist of highly personal information ranging from social security and insurance details to

specific medical diagnoses, lab results and treatment plans. Lack of immediate access to EMRs could cause chaos in hospitals that rely on these data for most of their operations.

In 2017, healthcare facilities in over 150 countries were attacked by WannaCry ransomware. This attack targeted unpatched Windows 7 operating systems with a specific vulnerability that allowed the attack to spread automatically across many systems. Britain's National Health Service (NHS) hospitals were among those particularly affected. Ransomware locked down the use of EMRs, and demanded a payment in bitcoin roughly equivalent to $300 per computer at the time. Reportedly, in England, 6,912 doctors' appointments (including critical operations) had to be cancelled as a result, and approximately 19,000 appointments were affected in some way (BBC News 2017). Five acute care hospitals had to divert emergency ambulances to other nearby hospitals (Morse 2017).

Shortly after WannaCry caused major disruption across healthcare systems, McAfee, a leading provider of antivirus software, called the WannaCry ransomware 'pseudo-ransomware' (Ashford 2017). Pseudo-ransomware is malware used by hackers more interested in causing disruption than in collecting money. This appears to be true for WannaCry because the ransomware only collected about $150,000 in ransom payments. This is an astonishingly low amount for an attack impacting so many and such critical systems. Similar ransomware like CryptoWall was used to collected $325M in ransoms (Ashford 2017).

McAfee's hypothesis that WannaCry's hackers were more interested in disruption than financial gain was validated in December 2017. The US and UK governments publicly accused North Korea of unleashing the WannaCry malware to 'cause havoc and destruction' (Nakashima and Rucker 2017). Because there was not a financial motive behind the hack, we believe that cyber negotiation might have been an excellent defensive strategy during the course of this attack. Below we outline an ideal pre-, mid- and post-negotiation strategy that might have been used in response to WannaCry.

Pre-attack

Considering that WannaCry only affected unpatched Windows 7 vulnerabilities, the ideal pre-attack negotiation strategy would have been to constantly patch EMR operating systems using the latest security updates. The reality is that many system administrators in hospitals do not perform such updates and often fail to deploy obvious technical defences. Before the attack, NHS Digital performed on-site cybersecurity assessments of 88 of the NHS trusts. None passed the cybersecurity standards inspection (Hern 2017). As part of a pre-attack cyber negotiation strategy, back-ups of all EMRs should have been made in case systems were corrupted or disabled. Considering how few victims paid the ransom, we guess that back-ups of the EMRS were available. However, they were not readily accessible; hence, the disruption of hospital services was severe. Because of the large-scale nature of the attack against many NHS hospitals, it is unclear whether individual hospitals had cyber incident response plans in place. The NHS had issued general guidance on how to handle such attacks, but it was not locally tested (Birdsey 2017). Considering the level of disruption, we assume that even if there were a plan in place for certain hospitals, it was poorly executed. We also surmise – based on how widespread the ransomware attack was – that formal communication pathways were not followed to ensure that awareness of the attack quickly moved up the organisational ladder and definitive instructions came back down. Further, it is clear that that

proper awareness was not built across the NHS employee base regarding possible phishing attacks because for the ransomware to be successfully installed an employee had to click on the infected link.

The attack

North Korea, the alleged WannaCry attackers, weaponized an exploit originally developed by the US National Security Agency (NSA) and released to the public by a cybercrime group called the Shadow Brokers. North Korea allegedly released the attack and then hired a third-party managed services team to facilitate the ransomware 'customer' (aka victim) support encrypted chat to help victims purchase bitcoin and understand how to get their data back (Ashford 2017). One reason a third-party team was hired to manage the attack could have been to obfuscate the fact North Korea launched it – providing a veil of anonymity.

When the attack was launched, it is unclear whether the hospitals involved convened an incident command team. Some likely did and determined that the attack posed very serious risks, considering hospital services were shut down entirely at numerous hospitals. Because of the high level of regulation surrounding national hospitals, legal teams were certainly convened to address the liability posed by the ransomware attack. While it is unclear if any hospitals negotiated directly with the hackers, there was an opportunity to do so. During the WannaCry attack, a McAfee security researcher asked the ransomware support operator via the customer support chat described above why the ransom was so low per machine. The operator responded that 'Those operating the ransomware had already been paid by someone to create and run the ransomware campaign to disrupt a competitor's business' (Ashford 2017). The defender could have used this information to their advantage considering it reveals the motive of the hacker (North Korea). Rather than paying the ransom, the defender might have argued that WannaCry had successfully disrupted their business. Thus, the attacker's objective was achieved. Depending on how much autonomy to negotiate the third party agency managing the ransomware has, such an argument could lead to a 'Good for You, Great for Me' scenario. The premise being that a negotiating partner can appreciate the goals of their negotiating partner and offer an outcome that achieves a good result while allowing their negotiating partner to achieve their minimum goal (Susskind 2014). In this case, the 'Good for You, Great for Me' scenario would have entailed North Korea hearing that they had successfully disrupted the hospital's operations, causing substantial damage, while the hospital received the decryption key it needed to unlock its EMRs and resume business without paying a ransom.

WannaCry illustrates the urgency of understanding the motives of an attacker in advance of any effort at cyber negotiation. If engagement with a hacker's agent or emissary is possible, and the right questions are asked, it may be possible to achieve a satisfying outcome, avoiding considerable financial and operational losses.

Post attack

After the WannaCry attack, unlike the Uber attack, the NHS carefully studied the impact the attack had on individual hospitals and the NHS's overall system. It developed a post-mortem attack report. From this analysis, documented in a National Audit Office report, several lessons were drawn and actions were recommended to improve future readiness and response to cyberattacks. These ranged from developing a response plan for the NHS

to follow in the case of future cyberattacks, especially to ensure that security updates and alerts are taken seriously and deployed immediately. The report, including lessons learned, was publicly shared for all to see. Further, NHS England and NHS Improvement are working with major trauma centres to allocate $21 million in capital funding to achieve cybersecurity enhancement (Morse 2017). This funding will be going to develop a security operations centre (SOC) for the NHS at which all security-related incidents will be handled.

These actions should improve the NHS's negotiation posture and help to foster a more resilient cybersecurity culture. Also, the widespread announcement of the lessons learned by the NHS shows the public and hackers that the attack was taken seriously and that the NHS will be better prepared in the future. This could be the best way to dissuade attackers from targeting the NHS, given that these measures have ameliorated obvious weaknesses that other hackers might exploit.

Future work

Our interviews provide a clear indication that it helps to think about cyberattacks and responses to them in terms of the three-phase negotiation framework we have identified. By collecting additional interviews from urban critical infrastructure operators, we hope to refine the framework and our prescriptions further. Our ambition is to develop a comprehensive cyber negotiation playbook with the help of an international advisory group. The kind of person we hope to invite to serve on this panel is someone like Moti Crystal, an Israeli negotiation expert who has been actively involved in urban critical infrastructure negotiation in many parts of the world. In addition, we hope that Chris Voss and others who helped to develop the FBI's Hostage Negotiation Manual will agree to participate. Finally, we plan to tap senior members of the many Crisis Negotiation teams managed by big city police departments throughout the world. In the same way that hostage negotiation has become a skill that every major city and country needs to have available, and trained negotiators have a well-documented playbook they can use (that builds on carefully assembled social science findings), we believe that helping every urban critical infrastructure manager prepare properly for cyber negotiations even if they have no intention of paying ransom is an important goal.

Conclusion

Urban critical infrastructure is composed of complex systems that do not warrant a 'Band-Aid' technology solution to cybersecurity challenges. Based on our interviews and case studies we are convinced that non-technical, defensive social engineering strategies such as employing a cyber negotiation process can be used to mitigate cyber risk for urban critical infrastructure. While we propose a series of negotiation steps that can be used to address urban critical infrastructure cyber risk management as summarised in Table 1, we have learned from our interviewees that it is important to not treat cybersecurity exclusively as a checkbox exercise where operators can pick and choose what steps are needed. Operationalising the entire cyber negotiation process is important to bolster organisational cyber resilience.

Cyber resilience is the notion that attacks will inevitably occur and impact the organisation in some way but that operations can continue with limited interruption. Today,

Table 1. Cyber negotiation process.

Cyber negotiation process		
Pre-attack	Attack	Post-attack
• Develop a cyber incident response plan	• Convene the incident command structure	• Develop a post-mortem attack report
• Build awareness	• Determine event severity	• Share information
• Deploy technical defences	• Consult the legal team	• Document lessons learned
• Formalise communication channels	• Negotiate	• Conduct external reputational damage control
• Establish external organisational relationships		

operators seem to give little attention to establishing a comprehensive cyber resilience strategy for urban critical infrastructure because operators are too busy battling daily operational challenges. To enable cyber resilience, operators should consider the following:

(1) Spend time and money identifying the likely costs and impacts if they lose control of their systems for any length of time. This will allow them to see that it is worth investing in system adaptation and enhance resilience;
(2) Make sure that the steps aimed at enhancing the resilience of systems after they are attacked are built into basic and continuing management operations. Adequate funds need to be set aside to add system redundancy so that hacked systems can be replaced immediately by parallel systems, or else resilience is just a pipe dream;
(3) Continuously train relevant staff regarding emergency response protocols so that everyone knows what to do when systems are compromised. An emergency response plan is useless if continuous training is not supported; and
(4) Formulate cyberattack emergency response plans with other agencies and levels of government so that efforts to implement these plans at a critical moment are not thwarted by countervailing efforts that have not been worked out in concert.

Resilience is a product of planning, preparation (training), investment in redundancy and forging working relationships with relevant partners and regulators.

The cyber negotiation process overlaps with actions needed to enhance resilience in the face of cyberattack – pre-planning to be sure that lines of authority are clear, putting an analytic capacity in place so that decisions can be made on whether it is worth paying a ransom, rehearsal or capacity-building so that negotiation procedures are ready to go, and added redundancy of systems so that agencies attacked have a better alternative to no agreement (BATNA). We hope that until comprehensive cyber resilience strategies become widely adopted, urban critical infrastructure operators can immediately begin to leverage our social-science-driven recommendations for addressing their infrastructure's cyber risk. All critical infrastructure managers should invest as much time, energy and money in Defensive Social Engineering as they do in technical defences to improve their organisation's cyber resilience.

Note

1. GDPR is a regulation that replaces the Data Protection Directive established in 1995. The Data Protection Directive set a minimum level of requirements concerning personal data privacy, and in 2012 the directive was recommended for overhaul based on the modern digital age. The GDPR is a more robust mechanism to protect data privacy built for today's pervasive technology environment. In addition to reinforcing previous data privacy rights, the GDPR provides the right to data portability, the right not be profiled using your data, and the right to be forgotten, among others. GDPR also requires large-scale private and public organisations to appoint a Data Protection Officer to ensure compliance with GDPR (European Data Protection Supervisor. 2018). GDPR requires data protection for all EU citizens, regardless of where the data is stored or where the company is based. Perhaps the most impactful component of GDPR is that there will be fines and penalties levied for non-compliance.

Acknowledgements

The authors would like to thank the Internet Policy Research Initiative (IPRI) at the Massachusetts Institute of Technology for funding this important effort. The authors would also like to thank Adam Hasz for his contributions to the study of Defensive Social Engineering and our broader research effort. Finally, the authors would like to thank the urban critical infrastructure operators who agreed to be interviewed for this research and for reviewing the manuscript.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

The work was funded by the Internet Policy Research Initiative @ MIT.

Notes on contributors

Gregory Falco is a hacker and critical infrastructure cybersecurity expert. He is a postdoctoral scholar at MIT's CSAIL and Stanford's FSI having earned his PhD from MIT in Cybersecurity, Urban Science and Infrastructure Management.

Alicia Noriega is an energy infrastructure expert having earned her Masters in Urban Planning, Environmental Policy and Energy Planning from MIT's DUSP.

Lawrence Susskind is the Ford Professor of Environmental and Urban Planning at MIT's DUSP. He was one of the Co-founders of the interuniversity Program on Negotiation at Harvard Law School, where he now directs the MIT-Harvard Public Negotiations Program, serves as Vice Chair for Education, and co-directs the Negotiation Pedagogy Initiative.

ORCID

Gregory Falco http://orcid.org/0000-0002-6463-7719

References

Ashford, Warwick. 2017. "Wannacry an Example of Pseudo-Ransomware, Says McAfee". *ComputerWeekly*. Accessed December 31, 2017. https://www.computerweekly.com/news/450427114/WannaCry-an-example-of-pseudo-ransomware-says-McAfee.

Assante, Michael, and Andrew Bochman. 2017. "Automation, Autonomy & Megacities 2025: A Dark Preview." *Center for Strategic and International Studies* 3: 1–16.
Atlanta Department of Procurement. 2018. "Emergency Procurements". Accessed May 5, 2018. https://procurement.atlantaga.gov/emergency-procurements/.
BBC News. 2017. "NHS Trusts 'At Fault' Over Cyber-Attack". *BBC News*. Accessed December 31, 2017. https://www.bbc.co.uk/news/technology-41753022.
Benner, Katie, Mike Isaac, and Sheera Frenkel. 2017. "Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data". *New York Times*, November 21. Accessed January 14, 2018. https://www.nytimes.com/2017/11/21/technology/uber-hack.html.
Berkeley. 2018. "Incident Response Planning Guideline – Information Security and Policy". Security Berkeley. Accessed February 24, 2018. https://security.berkeley.edu/incident-response-planning-guideline.
Berry, Melissa. 2017. "How Many Uber Drivers Are There? The Rideshare Guy Blog and Podcast". Accessed December 30, 2017. https://therideshareguy.com/how-many-uber-drivers-are-there/.
Birdsey, Ian. 2017. "NHS Cyber Incident Response Plan Not Tested Locally Prior To 'WannaCry' Attack, NAO Finds". *Out-Law*. Accessed April 9, 2018. https://www.out-law.com/en/articles/2017/october/nhs-cyber-incident-response-plan-not-tested-locally-prior-to-wannacry-attack-nao-finds/.
Carbon Black. 2017. *The Ransomware Economy*. Waltham: Carbon Black. Accessed November 9, 2017. https://www.carbonblack.com/resource/the-ransomware-economy/.
Cohen, Fred. 2006. *The Use of Deception Techniques: Honeypots and Decoys. Handbook of Information Security*. John Wiley & Sons.
Das, Samburaj. 2016. "Melrose Police Pay 1 Bitcoin to Get Rid of Ransomware". *CCN*, March 1. Accessed January 13, 2018. https://www.ccn.com/melrose-police-pay-1-bitcoin-to-get-rid-of-ransomware.
Dutton, Yvonne, and Jon Bellish. 2014. "Refusing to Negotiate: Analyzing the Legality and Practicality of a Piracy Ransom Ban." *Cornell International Law Journal* 47: 299–329.
European Data Protection Supervisor. 2018. "The History of the General Data Protection Regulation". *EDPS Europe*. Accessed February 25, 2018. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
Falco, Gregory, Arun Viswanathan, Carlos Caldera, and Howard Shrobe. 2018. "A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities." *IEEE Access* 6: 48360–48373. doi: 10.1109/ACCESS.2018.2867556.
Finkle, Jim, and Heather Somerville. 2017. "Regulators to Press Uber after it Admits Covering Up Data Breach". *Reuters*. Accessed December 31, 2017. https://www.reuters.com/article/us-uber-cyberattack/regulators-to-press-uber-after-it-admits-covering-up-data-breach-idUSKBN1DL2UQ.
F-Secure. 2016. "Evaluating the Customer Journey of Crypto-Ransomware and the Paradox Behind it". *Cyentia Institute*. Accessed February 26, 2018. https://www.cyentia.com/library-item/evaluating-the-customer-journey-of-crypto-ransomware-and-the-paradox-behind-it/.
Greenberg, Andy. 2017. "Uber Paid Off Hackers to Hide A 57-Million User Data Breach". *Wired*. Accessed December 30, 2017. https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/.
Greenemeier, Larry. 2018. "Urban Bungle: Atlanta Cyber Attack Puts Other Cities on Notice". *Scientific American*. Accessed May 5, 2018. https://www.scientificamerican.com/article/urban-bungle-atlanta-cyber-attack-puts-other-cities-on-notice/.
Hern, Alex. 2017. "NHS Could Have Avoided WannaCry Hack with 'Basic IT Security', Says Report". *Guardian*, October 27. Accessed December 31, 2017. https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office.
IBM. 2016. "IBM Study: Businesses More Likely to Pay Ransomware than Consumers". *IBM*. Accessed October 29, 2017. https://www-03.ibm.com/press/us/en/pressrelease/51230.wss.
INL. 2018. "Control Systems Cyber Security". Idaho National Laboratory. Accessed February 24, 2018. https://inl.gov/research-programs/control-systems-cyber-security/.
Jayaswal, Vikas, William Yurcik, and David Doss. 2002. "Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?" *Technology and Society* 380–386.
Klein, Andy. 2017. "Back-up Awareness Survey, Our 10th Year". Industry Report. Accessed October 31, 2017. https://www.backblaze.com/blog/back-up-awareness-survey/.

Köszegi, Sabine T., Gregory E. Kersten, and Rudolf Vetschera. 2002. "The Effects of Culture in Anonymous Negotiations: Experiment in Four Countries." *HICSS. Proceedings of the 35th Annual Hawaii International Conference*, 418–427.

Krebs, Brian. 2016. "San Francisco Rail System Hacker Hacked". Krebs on Security. Accessed October 31, 2017. https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/.

Lanceley, Frederick J. 2003. *On-Scene Guide for Crisis Negotiators*. Boca Raton: CRC Press.

Lennox-Gentle, Thaine. 2010. "Piracy, Sea Robbery, and Terrorism: Enforcing Laws to Deter Ransom Payments and Hijacking." *Transportation Law Journal* 37: 199–217.

Lynley, Matthew. 2017. "Travis Kalanick Says Uber Has 40 Million Monthly Active Riders". *TechCrunch*. Accessed December 30, 2017. https://techcrunch.com/2016/10/19/travis-kalanick-says-uber-has-40-million-monthly-active-riders/?guccounter=1.

Mansfield-Devine, Steve. 2016. "Ransomware: Taking Businesses Hostage." *Network Security* 2016 (10): 8–17. doi:10.1016/S1353-4858(16)30096-4.

McAfee. 2018. "Security Solutions: Endpoint, Cloud, Network, Antivirus, Malware". McAfee. Accessed December 31, 2017. https://www.mcafee.com/en-gb/index.html.

McCallister, Doreen. 2018. "Atlanta Working 'Around the Clock' to Fight Off Ransomware Attack." National Public Radio. Accessed May 5, 2018. https://www.npr.org/sections/thetwo-way/2018/03/27/597208778/atlanta-working-around-the-clock-to-fight-off-ransomware-attack?t=1549373586105.

Meyer, David. 2017. "Uber Is Already Getting Sued Over Its Gigantic Data Breach". *Fortune*. Accessed December 31, 2017. http://fortune.com/2017/11/22/uber-data-breach-lawsuit/.

Morse, Amyas. 2017. *Investigation: WannaCry Cyber Attack and the NHS*. London: National Audit Office. Accessed December 31, 2017. https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

Mozy. 2018. "Online Backup, Cloud Backup, and Data Backup Solutions". Mozy. Accessed December 31, 2017. https://mozy.co.uk/#slide-11.

Nakashima, Ellen, and Philip Rucker. 2017. "U.S. Declares North Korea Carried Out Massive WannaCry Cyberattack". *Washington Post*, December 19. Accessed December 31, 2017. https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html?noredirect=on&utm_term=.c761406ffdb5.

Newcomer, Eric. 2017. "Uber Paid Hackers to Delete Stolen Data on 57 Million People". Bloomberg. Accessed December 30, 2017. https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.

Orcutt, Mike. 2017. "Insurance Companies Are Struggling to Make Sense of Cybersecurity Risk". MIT Technology Review. Accessed February 28, 2018. https://lifeboat.com/blog/2017/04/insurance-companies-are-struggling-to-make-sense-of-cybersecurity-risk.

Palo Alto Networks. 2018. "Next Generation Security Platforms". Palo Alto Networks. Accessed October 31, 2017. https://paloaltonetworks.com.

Rodriguez, Joe. 2016. "Munis Tech Expert Reveals Details of Harrowing Ransomware Attack". *San Francisco Examiner*. Accessed October 31, 2017. http://www.sfexaminer.com/munis-tech-expert-reveals-details-harrowing-ransomware-attack/.

Stouffer, Keith, Joe Falco, and Karen Scarfone. 2011. "Guide to Industrial Control Systems (ICS) Security." *NIST Special Publication* 800 (82). doi:10.6028/NIST.SP.800-82r2.

Susskind, Lawrence. 2014. *Good for You, Great for Me: Finding the Trading Zone and Winning at Win-win Negotiation*. New York: Public Affairs.

Vecchi, Gregory M., Vincent B. Van Hasselt, and Stephen J. Romano. 2005. "Crisis (Hostage) Negotiation: Current Strategies and Issues in High-Risk Conflict Resolution." *Aggression and Violent Behavior* 10 (5): 533–551. doi:org/10.1016/j.avb.2004.10.001.

Williams, Clarence. 2017. "Hackers Hit D.C. Police Closed-Circuit Camera Network, City Officials Disclose". *Washington Post*, January 27. Accessed March 20, 2017. https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.402190c11df6.

Appendix A

Simulation screens and associated questions

Question 1:

- Do you have a cyberattack response plan in place for your organisation?
- Can you describe it?
- Is it different from your regular crisis response plan?

Question 2:

- What, if any, technologies do you employ to fend off hackers?

Question 3:

- What, if any, non-technical strategies do you use to fend off hackers?

Question 4:

- Have you checked to see if your systems are public on Shodan?

Simulation screen 1: You see someone has run a port scan against your system (Figure A1):
Question 5:

- Do you respond to this?

- If so, how?

Question 6:

- What technical strategies might you deploy?

Question 7:

- What non-technical strategies might you prepare?

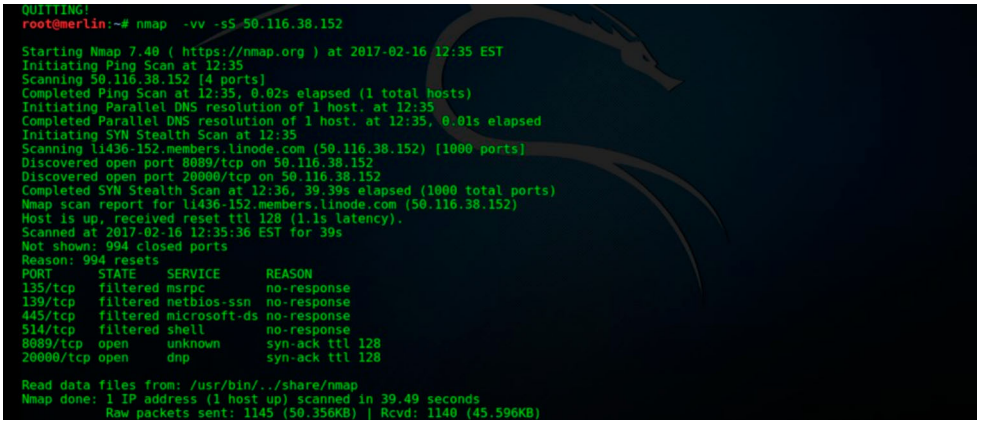

Figure A1. Port scanning screenshot.

Figure A2. Ransomware simulation screen.

Simulation screen 2: Shortly afterwards, one of your operator consoles shows the following attack (Figure A2):
Question 8:

- How, if at all, do you respond?

Question 9:

- If a hacker offered an opportunity to negotiate for the ransom, how would you advise others to proceed?

Question 10:

- Please describe your negotiation strategy.

Question 11:

- Would you advise others to handle these negotiations themselves?
- Or should they have an arrangement in place that would hand these negotiations over to someone else?

Question 12:

- Have you ever experienced a ransomware attack?
- What can you tell me about the experience?

Simulation screen 3: The attack has just ended (Figure A3):
Question 13:

- Who would the organisation turn to create a post-mortem of the attack?

Question 14:

- What kind of 'after-action' data gathering and discussion might occur?

Figure A3. Ransomware simulation screen.

Question 15:

- Who would have responsibility for deciding what the organisation learned from the experience?

Question 16:

- Will your organisation approach attack preparation differently now that you have been attacked?

Question 17:

- What type of damage control will need to be done?