Government Information Quarterly 39 (2022) 101703



Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf





Determinants of cyber-incidents among small and medium US cities

Mattia Caldarulo *, Eric W. Welch, Mary K. Feeney

Center for Science, Technology and Environmental Policy Studies (CSTEPS), School of Public Affairs, Arizona State University, USA

ARTICLE INFO

Keywords:
Cybersecurity
Cyber-incidents
Cybercrime
Security breaches
Unauthorized data disclosures
Routine activity theory

ABSTRACT

Cyber-incidents threaten the confidentiality, efficiency, and integrity of digital information systems, causing privacy risks, economic losses, and reputational damages, and exposing managerial limitations. Although these phenomena are becoming more frequent in public agencies, research to date has mainly focused on private sector organizations and individuals. In this study, we contribute to the broader literature on cyber-incidents by exploring the drivers of both security breaches and unauthorized data disclosures in public organizations. Drawing from routine activity theory, we develop hypotheses on the determinants of cyber-incidents in departments in small and medium-sized US cities and test them using data from a national survey of public managers. Our findings suggest that both environmental and organizational factors are key determinants of cyber-incidents in city government. The results demonstrate the application of routine activity theory to public sector organizations and identify external and internal elements related to cyber-incidents in city government departments.

1. Introduction

Cyber-incidents are events "*that could jeopardize the confidentiality, integrity, or availability of digital information or information systems*" (DHS, 2019, p. 1). Whether purposeful or accidental, cyber-incidents are increasingly common in the public sector, causing economic losses and reputational damages (GAO, 2016). Cyber-incidents raise citizens' privacy concerns, which are closely related to both trust in government and intentions to use e-government services (Macmanus, Caruson, & McPhee, 2013; Thompson, Mullins, & Chongsutakawewong, 2020; Thompson, Ravindran, & Nicosia, 2015). Government has the highest number of reported cyber-incidents in any sector (Romanosky, 2016). In 2020, cyber incidents targeting public organizations cost US taxpayers 8.64 million dollars in damages (IBM Security, 2020). However, most managers working in government (i.e., public managers), especially at the local level (e.g. cities and municipalities), have little understanding about when or why events such as hacking or ransoms occur (Caruson, Macmanus, & McPhee, 2012). Cyber-incidents have mostly been studied at the individual level or in private sector organizations (Holt & Bossler, 2016) and to a lesser extent on national governments (Macmanus et al., 2013; Norris, Mateczun, Joshi, & Finin, 2019; Thompson et al., 2020). This research responds to calls for a cross-disciplinary approach to study and understand cyber-incidents in cities (Preis & Susskind, 2020). We integrate organizational and community scholarship with routine activity theory (Cohen & Felson, 1979), to answer the following research question: How do organizational and environmental elements influence the likelihood that city government departments experience cyber-incidents?

Routine activity theory (RAT) is a dominant theoretical framework used to study cyber-incidents and cybercrime (Cohen & Felson, 1979). Developed originally to show that crime occurs when motivated offenders, suitable targets, and lack of guardians converge in time and space (Cohen & Felson, 1979), RAT has been adapted to explain a wide variety of cyber- incidents including phishing, online harassment, bullying, and fraud (Leukfeldt & Yar, 2016). For example, Reyns, Henson, and Fisher (2011) showed that RAT tenets of visibility, accessibility, and guardianship predict cyberstalking among college students. Holt, Leukfeldt, and Van De Weijer (2020) drew on RAT to explain the defacing of more than 130,000 Dutch websites. Most prior work applying RAT to cyber-incidents uses individuals or households as the unit of analysis without accounting for the environmental context due to unspecified connections between the physical world and cyberspace (Ife, Davies, Murdoch, & Stringhini, 2019; Yar, 2005).

In this study, we apply RAT to study cyber-incidents in city governments in the United States. In keeping with the original RAT design, we consider both organizational and environmental determinants of

* Corresponding author at: Center for Science, Technology and Environmental Policy Studies (CSTEPS), School of Public Affairs, Arizona State University, 411 N Central Ave #750, Phoenix, AZ 85004, USA.
E-mail address: mcaldaru@asu.edu (M. Caldarulo).

https://doi.org/10.1016/j.giq.2022.101703
Received 5 March 2021; Received in revised form 25 October 2021; Accepted 27 March 2022
Available online 13 April 2022
0740-624X/© 2022 Elsevier Inc. All rights reserved.

cyber-incidents in government departments in cities. We expect organizational factors, such as structure, culture, and IT capabilities of city departments to condition the occurrence of cyber-incidents. Specifically, we expect departments that are less professionalized, more decentralized, and have more risk-averse cultures to be more likely to experience cyber-incidents. We also expect political and societal factors, which comprise the environmental context, will explain exposure and vulnerability of city departments. For example, we anticipate that government organizations situated in more politicized and socially heterogeneous contexts, which are usually related to higher degrees of complexity and conflict, will be positively linked with cyber-incident occurrence.

To test our hypotheses, we estimate two cyber-incident models assessing security breaches and unauthorized releases of data. Our data come from a national survey administered in 2018 to public managers in 500 small and medium-sized US cities. Our study contributes to the literature by extending the application of RAT to US cities and by integrating the environmental components of RAT to explain cyber-incidents in city departments. Results inform public managers about the internal and external correlates of cyber-incidents.

In the next section, we outline the relevant literature and main constructs of our theoretical framework. We then cover hypotheses, data, methods, and results. We conclude with a discussion of the implications for research and practice.

2. Applying routine activity theory to study public sector cyber-incidents

Literature drawing on RAT to explain cyberattacks has mostly focused on individuals, with less research investigating public organizations as targets of cyber-incidents. We contend that the characteristics and contexts of cities make RAT a suitable theoretical framework for understanding cyber-incidents experienced by city departments.

Although cities have always been a key element in US political, social, and economic life, they have become even more relevant because of the rising urbanization, the increasing interconnectedness characterizing public sector organizations, and the ongoing emergence of smart cities and the Internet of Things (IoT) technologies, which made them key nodes of national IT networks and repositories of enormous quantities of sensitive data (Funk, Martin, DuPuis, Shark, & Bowen, 2019; Isett, Mergel, LeRoux, Mischen, & Rethemeyer, 2011; Preis & Susskind, 2020). Despite the growing importance and size of city information systems, few requirements and standards have been imposed by US state and federal laws to protect city IT systems (Preis & Susskind, 2020). Moreover, managers and employees in city departments often lack the competencies required to defend IT systems (Funk et al., 2019; Preis & Susskind, 2020). These features make city departments suitable and unguarded targets for offenders motivated by economic, social, and political reasons. That is, city departments are entities where offenders, targets, and lack of guardianship converge in time and space, making RAT an appropriate theoretical framework for studying cyber-incidents targeting them.

The first element that both cities and RAT victims have in common is the presence of **motivated offenders**. Motivated offenders are individuals or organizations that have criminal inclinations and the skills to commit a crime. Offenders targeting cities may be driven by several motives. Cities operate in dynamic environments, interact with numerous actors (e.g., ordinary citizens, contractors, other cities, or state and federal agencies), and often intervene to balance competing interests and values. This complexity may lead to economic, social, and political conflict and the emergence of offenders intent on creating disorder or destruction. Moreover, cities are often repositories of personally identifiable information such as police and financial records, which may entice criminal activity. Although there are various motives driving offenders, RAT assumes there will always be someone willing to commit a crime (Cohen & Felson, 1979).

RAT posits that motivated offenders are either internal or external to the organization (Handlington, 2018). Internal offenders can be malicious actors, motivated by the perspective of financial and personal gains, or accidental actors who compromise security without malicious intent (Handlington, 2018). Examples of malicious actors operating against city IT systems include employees that engage in data manipulation or fabrication for political gain or steal or sell data for financial gain. Accidental actors include employees or users who unintentionally damage the integrity of digital systems by downloading malicious software or releasing private data. External actors are nearly always categorized as malicious. Examples of external actors targeting city information systems include offenders with economic and terrorist intentions as well as "hacktivists" political protesters operating online (Brewster, Kemp, Galehbakhtiari, & Akhgar, 2015).

A **suitable target** is the second element of crime prediction outlined by RAT. Suitable targets have four main features: value, inertia, visibility, and accessibility (VIVA) (Cohen & Felson, 1979). *Value* in the cyberworld can be conceptualized in two distinct ways: the intrinsic value of the target and the value placed upon it. Offenders might violate an IT system because it has data worth millions of dollars (e.g. passwords to bank accounts) or because it is connected to an organizational intranet. In the first case, the value of the target lies in its intrinsic features. In the second case, the target is valuable as a gateway to other information systems. Literature on cybercrime mostly investigates the intrinsic value of targets (Jansen & Leukfeldt, 2016; Leukfeldt & Yar, 2016). City departments could be targeted both because they store sensitive information and because of their connectedness with other organizations. For example, police departments may be considered valuable targets because they produce individual records and because of their continuous interaction with other departments and agencies (e.g., DMV and FBI).

Inertia refers to the physical presence or characteristics of the target that impede its removal, steal, or disruption. Among the four features of the VIVA framework, inertia is the least studied and not typically applied to the cyberworld. Leukfeldt and Yar (2016) suggest that inertia is not relevant to cyberspace because there is no physical property with weight or height constraints to increase or decrease the likelihood of theft. Although cyberspace does not have physical properties of weight and height, organizational inertia may influence the likelihood of cyberattacks. City departments, which produce information-loaded products and have political purposes, are required to be reliable and accountable (Hannan & Freeman, 1984). These demands lead to pressures to create reproducible activities and structures which may generate strong structural inertia, halting changes in organizational technologies (Hannan & Freeman, 1984; Lindblom, 1959). Infrastructure investments, sunk costs, outdated conceptual frameworks, and mismatched employee skills may prevent change and implementation of new cybersecurity policies (Hannan & Freeman, 1984; Shively, 2021). As a consequence, at the organizational level, inertia could determine cyber-incidents.

The third feature of suitable targets is *visibility*. RAT predicts that the greater the visibility of a target, the greater the risk of crime occurrence (Cohen & Felson, 1979). Visibility is often instrumentalized as the amount of time individuals spend online and the activities they perform (Leukfeldt & Yar, 2016; Reyns et al., 2011). These measures, however, are less appropriate for studying the likelihood a city department would be targeted. Department visibility might be captured as the number of IT channels a department has. The greater the online presence of a city department, the greater its visibility and risk of cyber incidents.

Accessibility is the fourth VIVA feature. Accessible targets make it easy for offenders to commit the crime without being noticed. The cybercrime literature operationalizes accessibility by looking at a target's operating systems as some are more prone to cyberattacks (Reyns et al., 2011). Accessibility may also depend on the number of connections a department has with other actors. The greater the number of potential access points to a department's IT infrastructure, the more complex it is to monitor and secure. Increased interconnectedness

among city departments may increase exposure to cyber-incidents.

According to RAT, the third element predicting the likelihood of crime occurrence is the **lack of capable guardianship**. Capable guardians include technological (e.g. locks), social (e.g. neighborhood), and personal forms of security (e.g. individuals' skills) (Holt & Bossler, 2016). In the cyberworld, technological guardians are often associated with antivirus applications (Choi, 2008) or parental control software (Leukfeldt & Yar, 2016). Social guardianship can be thought of as organizational ability to recognize the weaknesses of existing cybersecurity policies (Conklin & White, 2006). Personal forms of security include individual computer skills, password management, and general digital literacy (Graham & Triplett, 2017). For city departments, capable guardians include skilled employees who are able to recognize suspect material like phishing messages (i.e., personal guardianship), public managers who develop IT policies (i.e., technological guardianship), and organizational controls and rules that enhance detection of system failures (i.e., social guardianship).

Although motivated offenders, suitable targets, and incapable guardians are necessary conditions for crime occurrence, they are not sufficient. Cohen and Felson (1979) argue that for crime to take place, the three elements must converge in space and time, requiring geographic proximity between the offender and the target. Even though the differences between the digital and physical worlds create challenges for the transposition of RAT to study cybercrimes (Jahankhani, Al-Nemrat, & Hosseinnian-Far, 2014; Yar, 2005), convincing arguments posit that geographical distance and physical content play an important role in cyberspace. For example, recent research has developed a framework that allows to integrate environmental criminology theories (e.g., RAT) to explain cyber-incidents (Ife et al., 2019). We adapt this work for our study of city departments, which simultaneously occupy and operate in cyber and physical spaces (e.g., defined boundaries for residency and in-person services), making it necessary to include characteristics about the locality and factors in a city's proximate geographic in order to predict the occurrence of cyber-incidents.

This research adapts RAT to explain cyber-incidents in city departments in three fundamental ways. First, we focus on cities departments, shifting the unit of analysis from the individual to the organization. Second, we follow prior research identifying the key elements of RAT – motivated offenders, suitable targets, capable guardianship – applying them at the organizational level. Third, we expand the way RAT is applied in the cyber-literature to include the organizational environment. This reintegrates an important theoretical dimension of RAT and fits public administration and organization research in which environmental factors are key to understanding organizational phenomena (Lawrence & Lorsch, 1967; Pfeffer & Salancik, 1978; Scott & Davis, 2007).

2.1. Organizational determinants

RAT argues that crime occurs when and where lack of capable guardians, motivated offenders, and suitable targets converge. We expect that organizational characteristics such as structure, risk propensity, points of access, and IT capacity influence both the suitability of public organizations as targets and the presence of guardianship determining cyber-incidents.

2.1.1. Centralization

Public sector organizations that have centralized structures tend to concentrate power and authority in a few hands, minimizing the involvement of staff in decision-making processes (Andrews, Boyne, Law, & Walker, 2009; Rainey, 2009). Centralized public organizations are more likely to pursue successful entrepreneurship activities aimed at improving the organizational operational efficiency (Andrews et al., 2009; Moon, 1999). Research has found that centralized public organizations are characterized by lower levels of internal information sharing and higher levels of electronic monitoring intensity (Fusi & Feeney, 2018; Yang & Maxwell, 2011). Therefore, we expect that more centralized city departments will have fewer points of access and higher guardianship levels, which, according to RAT, should reduce the likelihood of cyber-incidents.

H_{1a}. City departments with more centralized decision-making structures are less likely to report experiencing cyber-incidents.

2.1.2. Risk-taking culture

Elements such as IT innovations, growth of IT budgets, and design of procedures to anticipate cyberattacks can help organizations to manage and respond to cyber threats (Caruson et al., 2012; Romanosky, 2016). Research finds a positive relationship between top-management risk propensity and IT innovativeness in public, private, and nonprofit organizations (Moon & Bretschneider, 2002). Consequently, city departments that are more prone to take risks are more likely to invest in IT solutions that act as guardians and ultimately minimize cyber threats. Risk-taking is also associated with lower levels of structural inertia, which hampers investments in information technologies and exposes organizations to cyber-incidents (Desai, 2008; Mikalef, van de Wetering, & Krogstie, 2021). City departments characterized by risk-taking cultures may therefore implement non-routine tasks and ideas which reduce organizational predictability and inertia, minimizing cyber-attacks (Bourgon, 2009; Terry, 1998).

H_{1b}. City departments with more risk-taking cultures are less likely to report experiencing cyber-incidents.

2.1.3. Points of access

Digital information channels (IT channels) are increasingly adopted by small and medium city departments to enhance internal and external communication and coordination (Feeney, Fusi, Camarena, & Zhang, 2019). This widespread adoption stems from the increasing interdependencies of public organizations (Isett et al., 2011) requiring even small cities to cooperate within and between governmental levels. Social media such as Facebook and Twitter enable departments to provide timely information to citizens, software like Dropbox allows teams to store, share, and collaborate on documents. IT channels represent access points which, according to RAT, increase the likelihood of cyber-incidents. The more access points an organization has, the greater the number of paths by which an offender could access it (Beavon, Brantingham, & Brantingham, 1994). In US cities, the adoption of IT channels is usually associated with increased data reception from external stakeholders (Fusi & Feeney, 2020), a feature that might expose departments to threats from external offenders. Additionally, having numerous digital information channels through which organizations interact with other participants in the administrative process (both internal and external to the organization) will strain guardianship and result in more cyber-incidents (Cohen & Felson, 1979). Multiple points of access increase the probability that internal actors disclose sensitive information accidentally or on purpose. Moreover, multiple IT channels signal a potential richness of data and information, which from a RAT perspective would both increase the value and the accessibility of the target.

H_{1c}. City departments that have more IT channels are more likely to report experiencing cyber-incidents.

2.1.4. IT capacity

RAT suggests that the lack of capable guardians encourages crime occurrence (Cohen & Felson, 1979). Organizations willing to enhance their cyber-guardianship can invest in both technology and human capital, ensuring that employees develop the skills and have the tools to prevent, detect, and respond to cyber-incidents (Caruson et al., 2012). Yet research finds great variation in US cities' technical capacity (Feeney et al., 2019). For example, Norris et al. (2019) show that US cities vary in preparedness to detect, prevent, and recover from different types of

cyber threats. Feeney and Brown (2017) find that variation in city technology use and digital infrastructure is related to city size and whether organizations have internal IT departments or contract out services. Given the importance of IT capacity in e-government development and capable guardianship, we expect IT capacity to increase cybersecurity and reduce cyber-incidents (Caruson et al., 2012).

H_{1d}. City departments with higher levels of IT capacity are less likely to report experiencing cyber-incidents.

2.2. Environmental determinants

Research suggests the environment plays a key role in influencing both crime occurrence and public sector organizational behavior (Cohen & Felson, 1979; Fusi & Feeney, 2020; Hipp, 2007). RAT argues that the spatial convergence of motivated offenders, suitable targets, and lack of capable guardianship determines crime. We expect that environmental elements such as the form of government of a city, level of political competition, economic and racial heterogeneity, and population size will influence the emergence of offenders, the suitability of departments as targets, and the presence of guardianship.

2.2.1. Political factors

We expect that cyber-incidents will be related to political structure and competition in the environment where city departments operate. There are two main forms of government in US cities: mayor-council and council-manager. Mayor-council governments are led by elected representatives and are generally more political than council-manager governments which are a combination of elected officials (the council) and professional staff (the manager). Council-manager cities are typically more professionalized (Carr, 2015), more likely to adopt and use ICTs for public participation (Zhang & Feeney, 2020), and have a higher capacity for technology management and e-government services (Feeney et al., 2019). It is therefore reasonable to expect that council-manager governments will have more effective and capable guardians (either technological, social, or personal) to prevent cyber-incidents. Mayor-council cities are more politicized and associated with higher levels of political conflict, managerial turnover, and political influence from lobbyists (Carr, 2015). These higher levels of political conflict are likely to result in more motivated offenders and, thus, greater likelihood of cyber-incidents.

H_{2a}. Departments in cities with a council-manager form of government will be less likely to report experiencing cyber-incidents than those in mayor-council cities.

We expect political competition in the environment to increase the likelihood of cyber-incidents. Political competition is positively associated with crime, in general. Political competition predicts diverse forms of racial violence and hate crimes (Olzak, 1990) and criminal organizations strategically use violence during election years, where political competition is fierce (Alesina, Piccolo, & Pinotti, 2019). Social, political, economic, and cultural conflicts are also associated with cyberattacks (Gandhi et al., 2011). While prior research does not point directly to evidence linking political competition and cyber-incidents, it suggests that political competition increases criminal motivations and may create a perception that organizations are weak, thus raising their visibility and value as suitable targets of disruption.

H_{2b}. Departments in cities with greater political competition are more likely to report experiencing cyber-incidents.

2.2.2. Social heterogeneity

The criminology literature shows income inequality is a strong antecedent of crime occurrence, even when controlling for competing hypotheses (Coccia, 2017). Income inequality is associated with personal crime, such as homicides (Coccia, 2017), and property crime (Metz & Burdina, 2018). Income inequality leads to a breakdown of social cohesion (Kennedy, Kawachi, Prothrow-Stith, Lochner, & Gupta, 1998), a rise in social conflict and discrimination (Coccia, 2017), and a surge in the number of motivated offenders (Maume, 1989), which increases crime occurrence. In the context of cybercrime, socioeconomic conditions in a community such as low education and income inequality moderate the relationship between internet adoption and cybercrime occurrence (Park, Cho, Lee, & Lee, 2019). Drawing from previous research on RAT elements and crime, we expect that when applying RAT to city departments, the economic conditions in a city will be positively related to the motivation of offenders and the level of guardianship of the IT system.

H_{2c}. Departments in cities characterized by higher levels of economic inequality are more likely to report experiencing cyber-incidents.

Racial heterogeneity in the US is positively associated with crime in cities (Hipp, 2007). Hipp (2007) reviews six theories, including RAT, describing the causal mechanisms between racial heterogeneity and crime. Most of these theories expect that the greater the heterogeneity in a community, the more likely there will be conflict. Structural inequality can destabilize core societal values, creating feelings of hostility (Hipp, 2007; Ousey & Lee, 2013). Conflict and hostility are positively related to deviant behaviors and crime occurrence (McCaghy, Capron, Jamieson, & Carey, 2008). When inequalities are perceived as illegitimate, individuals in disadvantaged groups are more likely to commit crimes to redistribute or fight for a larger share of resources (Hipp, 2007). When individuals who belong to an advantaged group feel that their privileges are threatened, they will defend their position through criminal activities (Hipp, 2007; Ousey & Lee, 2013). Racial inequalities play a role also in cyberspace (Graham, 2020; McCaghy et al., 2008). For instance, in May 2020 the Minneapolis police department website was targeted by hackers in response to the George Floyd killing (Ropek, 2020). We expect that highly visible and symbolic public organizations operating in racially heterogeneous environments will be suitable targets for motivated offenders who want to protest against or perpetuate racial inequalities, determining both external and internal cyber-incidents.

H_{2d}. Departments in cities characterized by higher levels of racial heterogeneity are more likely to report experiencing cyber-incidents.

2.2.3. Target size

According to RAT, the value of the target can trigger crime. Government organizations in larger cities have more resources, are more prominent, and have a larger trove of potentially valuable data. Since cyber-incidents in public organizations with larger data repositories cause greater damage and offer greater potential financial benefits to attackers (The Economist, 2017), larger cities will be more attractive (i.e. valuable) targets to those interested in disrupting information systems as well as to those seeking sensitive proprietary information.

H_{2e}. Departments in larger cities will be more likely to report experiencing cyber-incidents.

Fig. 1 illustrates our application of RAT to model the occurrence of cyber-incidents in city departments, noting organizational and environmental elements that align with RAT theory and predict relationships with the dependent variables. We expect four organizational elements and four environmental factors to be related to security breaches and unauthorized data disclosures. Among the organizational factors, we expect centralized organizations to be less likely to report experiencing cyber-incidents as they are associated with higher levels of electronic monitoring intensity (capable guardianship) and fewer access points (accessibility); risk propensity to be associated with both capable guardianship and lower levels of organizational inertia and, hence, less prone to reporting cyber-incidents; increased social media channels to make a department more accessible, vulnerable, and high value; and increased IT capacity to make city departments more capable guardians against cyber-incidents. From an environmental perspective, we expect

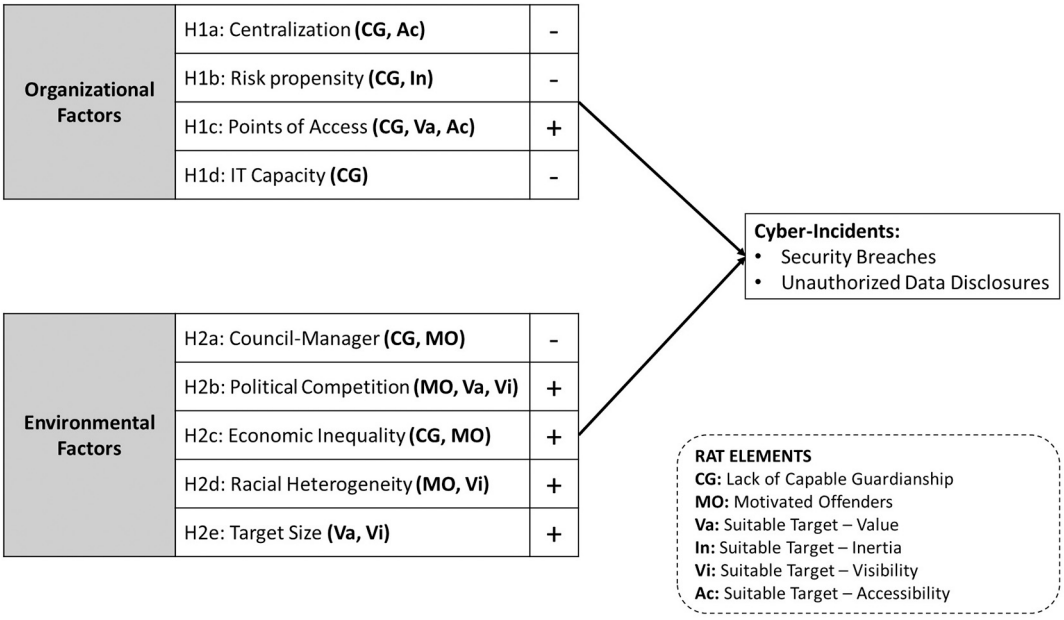


Fig. 1. Application of RAT to cyber-incidents in city government departments.

council-manager cities to be less likely to report experiencing cyber-incidents due to their greater technical expertise (capable guardianship) and lower levels of political conflicts (less motivated offenders); political competition and social heterogeneity to be associated with higher levels of conflict and visibility, hence, positively related to cyber-incidents occurrence; and city population to be positively related to cyber-incidents because of greater value and visibility.

3. Data and measures

3.1. Data

We draw on multiple sources of data to perform our analysis. Our primary source of cyber-incidents and organizational data is a Center for Science, Technology, and Environmental Policy Studies 2018 survey on technology use that was administered to department leaders in 500 small and medium-sized cities. The sample includes all 184 US cities with populations ranging from 100,000 to 250,000 and a random sample of 316 US cities with populations from 25,000 to 99,999. Data are weighted to account for the sampling approach. Surveys were administered to the director or deputy director of five departments in each city: police, community development, parks and recreation, Mayor's office, and finance. The survey was administered to an adjusted sample of 2228 individuals since ineligible cases (retired and no longer employed individuals) were removed from the initial sample. 621 usable responses were recorded for a response rate of 30%, calculated following AAPOR RR2 guidelines. The final dataset has 578 observations as 43 respondents who answered "I Don't Know" to all the questions related to data disclosure events that occurred in their organizations in the last 12 months were removed from the sample.

We merged the survey responses with administrative data including the 2017 American Community Survey 1-year county-level estimates, 2016 presidential election data from the New York Times, data from Social Explorer – an online tool providing access to governmental data in a user-friendly way – and political affiliation data from the National Governors Association.

3.2. Measures

3.2.1. Dependent variables

We test our hypotheses on two different types of cyber-incidents: security breaches and unauthorized data disclosures. Security breaches indicate cyber-incidents caused by external malicious offenders. Unauthorized data disclosures measure cyber-incidents caused by internal actors, which can be malicious or accidental.

The two dependent variables come from four items asking respondents if in the previous 12 months their organizations experienced (i) unauthorized disclosure of information to media, (ii) unauthorized disclosure of information to politicians or other key public officials, (iii) unauthorized disclosure of information to citizens or other community groups, (iv) security breaches from an external organization. Response categories to each item include 0 = no, 1 = yes, and 2 = I don't know (coded as missing).[1] The items derived from previous research characterizing "security breaches" and "unauthorized data disclosures". We conducted a factor analysis of the responses to empirically assess whether they capture distinct theoretical concepts. Results of the analysis show that there are two distinct concepts with eigenvalues are greater than 1. The first factor is composed of three "unauthorized disclosure" items. The second factor is composed of the single "security breach" item. Standardized factor loadings were all significant ($p < 0.00$) and greater than 0.75.

Responses to the security breach item represent the first outcome variable. Of the 578 respondents, less than half (45.25%) reported security breaches. "I don't know" answers are coded as missing.

We construct the second dependent variable by combining the responses to the three "unauthorized data disclosures" survey items. **Unauthorized data disclosures** is dichotomous and equal to one if managers experienced at least one form of unauthorized data disclosure. Around 10% of the respondents experienced at least one type of unauthorized data disclosure.

[1] Since cyber-incidents are usually extraordinary negative events remembered by officials (Ochsner, 2000), "Don't know" answers can indicate that an event has not occurred or has not been identified. Thus, we estimate identical models in which "don't know" responses are coded as "no" (i.e. 0). Since results are consistent, we only discuss the estimates having "don't know" answers coded as missing. Appendix A reports estimates for the alternative models.

3.2.2. Independent variables

We include four organizational variables: centralization, risk-taking culture, IT communication channels, and IT capacity. We measure **Centralization** by combining three items of the 2018 survey in an equally weighted index with a Cronbach's alpha of 0.63. Managers were asked their agreement with the following statements: "Top management exerts strong control over this organization"; "There can be little action taken here until a supervisor approves a decision" and "Even small matters have to be referred to someone higher up for a final answer" (Response categories: 5-point Likert scale 1 = strongly disagree to 5 = strongly agree).

The strength of risk-taking cultures is an index of three survey items asking the level of agreement (Response categories: 5-point Likert scale 1 = strongly disagree to 5 = strongly agree) with the following statements: (i) most employees in this organization are not afraid to take risks; (ii) this organization has a strong commitment to innovation. People who develop innovative solutions to problems are rewarded; and (iii) this organization is a very dynamic and entrepreneurial place. People are willing to stick their necks out and take risks. **Risk-taking Culture** has a Cronbach's alpha of 0.75.

To compute the number of **IT communication channels** in the organization, we asked respondents to indicate if they use the following tools for work purposes: Facebook; Twitter; YouTube; LinkedIn; Instagram; Document collaboration tools (e.g. Google Docs, Wikis); Work coordination tools (e.g. Google Calendar, MS Project, Slack); File sharing tools (e.g. Dropbox, Google Drive, Box.com). The resulting variable is a count of the number of technologies indicated by respondents.

IT Capacity is measured as an index from responses to four survey items: (i) "My agency is too busy to effectively monitor, control, and use the data we collect"; (ii) "There is a mismatch between our department's needs and what technology can provide"; (iii) "Management lacks software applications that would make work more efficient" and (iv) "My agency is ill-equipped to manage important questions about online security and privacy" (Response categories: 5-point Likert scale 1 = strongly disagree to 5 = strongly agree). The Cronbach's alpha for IT Capacity is 0.79.

At the environmental level, we include five variables: form of government, margin of partisan vote, party change in gubernatorial elections, economic inequality, racial heterogeneity, and target size. **Form of government** is a dichotomous variable coded one if a city has a council-manager form of government and zero if mayor-council.

Political competition is operationalized in two ways: margin of partisan vote at the county level and number of party changes in gubernatorial elections (Svaleryd & Vlachos, 2009). **Margin of partisan vote** is measured as indicated by Eq. 1:

$$MOV_{2016} = -|d_s - 0.5| \quad (1)$$

where MOV is the negative absolute value of the difference between the % of democratic votes in the 2016 presidential elections and 50%. Margin of partisan vote is a good proxy measure of swing voters especially when the vote density function is single-peaked, symmetrical, and there are only two parties (Svaleryd & Vlachos, 2009). Higher values of this measure indicate more political competition in a county. To compute margin of partisan vote, we use data from the New York Times.[2] Our second measure of political competition is **party change in gubernatorial elections** and indicates a higher number of swing voters and political competition in a state. Data are taken from the National Governors Association. Shifts are computed as the number of times a state flipped over the previous ten gubernatorial elections.

Gini coefficient measures **economic inequality** by reporting the difference between a perfectly equal income distribution and the actual income distribution. This index ranges from 0 to 1, the higher the greater the income concentration and, thus, inequality. Gini Coefficient data were downloaded from the 2017 ACS 1-year estimate.

We use Lieberson's (1969) **Index of Heterogeneity** as our measure of racial heterogeneity. The index determines diversity within a population by using the formula represented by Eq. 2:

$$A_w = 1 - \sum_{k=1}^{p} Y_k^2 \quad (2)$$

where Y_k is the proportion of the population identifying itself with a specific race category and p is the total number of categories. The higher the index, the more heterogeneous the population. We use data on eight racial groups from the 2017-ACS 1-year estimates data: White; Black and Afro American; Hispanic or Latino; American Indian and Alaska Native; Asian alone; Native Hawaiian and Other Pacific Islander; other race; and two or more races.

To measure **Target Size**, we use the natural logarithm of 2017 population data for each city.

3.2.3. Control variables

We include six control variables at the department and individual levels. Different types of departments may handle or have access to unique data, so we include five dummy variables for **department type** (police, community development, parks and recreation, Mayor's office, and finance). The size of the organization may be related to resources and the number of cyber threats and opportunities for cyber-incidents faced during an ordinary working day, so we control for **department size** (natural logarithm of the number of full-time employees).

Since we expect that **prior work experience in the private sector** might be related to knowledge about cybersecurity best practices, we also control for the number of years respondents worked in the private sector.

Table 1 presents the descriptive statistics for the variables and their sources. Correlations among variables are reported in Table 2.

4. Results

To test our hypotheses, we run two binary logistic regression models using R (v. 4.0.3) and clustering standard errors at the city level. The first model investigates the determinants of security breaches caused by external actors. The second model predicts unauthorized data disclosures occurrence. Variance inflation factors are below the threshold value of four, thus multicollinearity is not a concern (O'Brien, 2007).

Table 3 presents our results. We discuss findings related to each hypothesis and then consider implications and limitations in the conclusion.

4.1. Organizational determinants of cyber-incidents

Our models do not support Hypotheses 1a and 1b which predicted that departments with stronger risk-taking cultures and centralized decision-making structures, respectively, would be more likely to report experiencing cyber-incidents.

We find support for Hypothesis 1c. Departments with increased IT communication channels are more likely to report experiencing cyber-incidents. Average marginal effects indicate that an additional IT channel is associated with a 5.4% ($p < 0.01$) increase in the likelihood of reporting experiencing security breaches and a 1.2% ($p < 0.10$) increase in the likelihood of reporting unauthorized data disclosures.

Our results support Hypothesis 1d. City departments with higher levels of IT capacity are less likely to report experiencing cyber-incidents. Our findings show that a one-unit increase in IT capacity is associated with a 7.7% ($p < 0.05$) reduction in the probability of

[2] For six states (Connecticut, Massachusetts, Maine, New Hampshire, Rhode Island, and Vermont), whose data are not available at the county level on the New York Times, we use data taken from socialexplorer.com. Due to the lack of county-level data, for Alaska we use state-level data. For cities located across multiple counties, we average county data.

Table 1
Descriptive statistics.

Variable	N	Minimum	Maximum	Mean	Std. Deviation	Source
Dependent Variables						
Security Breaches	442	0	1	0.45	0.50	2018 Survey
Unauthorized Data Disclosures	529	0	1	0.10	0.30	2018 Survey
Independent Variable – Organizational Factors						
Centralization	555	1	5	2.48	0.68	2018 Survey
Risk-Taking	555	1	5	3.26	0.78	2018 Survey
Number of IT Communication Channels	578	0	8	4.84	2.13	2018 Survey
IT Capacity	572	1.25	5	3.41	0.86	2018 Survey
Independent Variable – Environmental Factors						
Form of Government	578	0	1	0.24	0.43	2018 Survey
Margin of Partisan Vote	578	−0.41	0	−0.12	0.09	nytimes.com, Social Explorer
# Partisan Shifts in the Last 10 Gubernatorial elections (ln)	576	0	1.79	1.02	0.42	National Governors Association
Gini Coefficient	560	0.37	0.55	0.46	0.03	2017 ACS 1 Year Estimates
Lieberson Index	551	0.14	0.75	0.53	0.14	2017 ACS 1 Year Estimates
Population (2017) (ln)	573	9.99	12.62	11.31	0.70	U.S. Census Bureau
Control Variables						
City Manager	578	0	1	0.17	0.37	2018 Survey
Director of Community	578	0	1	0.22	0.42	2018 Survey
Finance Department	578	0	1	0.20	0.40	2018 Survey
Parks Department	578	0	1	0.20	0.40	2018 Survey
Police Department	578	0	1	0.21	0.41	2018 Survey
Full-Time Employees (ln)	548	0	8.52	3.75	1.56	2018 Survey
Years of Experience in the Private Sector	546	0	42.00	5.00	6.25	2018 Survey

reporting security breaches and a 3.3% ($p < 0.05$) decrease in the likelihood of reporting unauthorized data disclosures.

4.2. Environmental determinants of cyber-incidents

We find partial support for Hypothesis 2a. Cities characterized by council-manager form of government are less likely to report experiencing cyber-incidents. The probability of reporting security breaches is 16.0% ($p < 0.05$) less for cities with a council-manager form of government as compared to those with mayor-council governments. We do not find a significant relationship between form of government and reporting occurrences of unauthorized data disclosures.

Hypothesis 2b expected a positive association between the level of political competition and reports of cyber-incidents. We find a negative and statistically significant relationship between the natural logarithm of the number of partisan shifts in the last 10 gubernatorial elections and security breaches reporting ($B = -0.488$; $p < 0.10$). Margin of partisan vote is not significantly related to reporting security breaches. Unauthorized data disclosures are not related to partisan shifts but positively associated with margin of partisan vote ($B = 3.221$; $p < 0.10$).

Our hypotheses relating cyber-incidents and social heterogeneity are not supported. Departments in cities with higher economic inequality (Hypothesis 2c), greater racial heterogeneity (Hypothesis 2d), and larger populations (Hypothesis 2e) are not more or less likely to report security breaches or unauthorized data disclosures.

The results provide preliminary insights on the elements that are related to the likelihood of cyber-incidents in public organizations, yet we acknowledge some limitations. First, managers' responses about cyber-incidents may be characterized by social desirability bias, though, research has shown that measuring organizational properties through self-reported data can provide valid results (Lincoln & Zeitz, 1980). Second, we use proxies to operationalize some of the key independent variables. For example, city population is a proxy for wealth and data capacity and complexity since smaller cities often lack the resources to provide the same levels of services offered by larger cities (Feeney et al., 2019; Mossberger, Wu, & Crawford, 2013). Third, it is possible that some managers may not have knowledge of cyber-incidents or that their responses were subject to social desirability biases, leading us to underestimate the pervasiveness of these phenomena. Cyber-incidents are extremely salient events, whose occurrences are difficult to hide from management. Although possible, it is unlikely that department heads are unaware of these events. Our choice of administering the survey online rather than in person, and ensuring respondents' confidentiality should have minimized social desirability biases (Fricker, Galesic, Tourangeau, & Yan, 2005). Additionally, because we use cross-sectional survey data, we cannot infer causality. Fifth, although we study two different types of cyber-incidents, our hypotheses do not distinguish between the two types of cyber-crime. Although this is consistent with other studies using RAT to investigate cyber-incidents (e.g., Ngo & Paternoster, 2011), future studies should further explore the relationship between the nature of cyber-incidents, their antecedents, and consequences. Last, our data do not allow us to measure the severity and the frequency of the cyber-incidents. Future research should develop measures to capture these dimensions and assess the extent to which public sector organizational and environmental factors influence the magnitude and the recurrence of cyber incidents.

5. Discussion

Our results suggest that among all the RAT elements capable guardianship is a key determinant of cyber-incidents in city departments, both at the organizational and environmental levels. At the organizational level, we find that greater IT capacity reduces the likelihood of reporting cyber-incidents. Similarly, more IT channels, which may constrain guardianship levels, are associated with both security breaches and unauthorized data disclosures experiences.

At the environmental level, we find that organizations that are more professional (i.e. council-managers cities) are less likely to report security breaches. This aligns with previous research findings that professionalized city governments produce more technology outcomes (Carr, 2015; Feeney et al., 2019; Zhang & Feeney, 2020). Taken together, our findings suggest that more professionally oriented departments that monitor their IT channels and invest in developing IT capacity are less prone to cyber-incidents, as it is possible that these organizations develop and put in place more effective prevention strategies for managing cyber threats.

We find a negative and significant relationship between the number of partisan shifts in the last 10 gubernatorial elections and the likelihood of experiencing security breaches and a positive and significant relationship between the margin of partisan vote and the likelihood of reporting unauthorized data disclosures. From a RAT perspective, these results confirm our expectation that the environmental aspects of the theory are important predictors of cyber-incidents in public organizations. Integrating environmental context is vital to understanding the

Table 2
Correlation matrix.

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Security Breaches	1																		
Unauthorized Data Disclosures	0.062	1																	
Council-Manager	−0.17**	0.01	1																
# Partisan Shifts in the Last 10 Gubernatorial elections (ln)	−0.07	0.06	0.02	1															
Margin of Partisan Vote	0.01	0.08	0.07	−0.05	1														
Gini Coefficient	−0.03	0.02	0.04	0.101*	−0.28**	1													
Lieberson Index of Inequality	−0.01	−0.02	−0.30**	0.04	−0.32**	0.370**	1												
Ln.Population (2017)	0.10*	0.118**	−0.083*	0.04	0.138**	0.05	0.230**	1											
Centralization	−0.004	0.08	0.127**	0.07	−0.06	0.103*	−0.03	−0.001	1										
Risk-Taking	0.02	−0.09	−0.15**	−0.12**	0.01	−0.105*	0.03	0.05	−0.43**	1									
Number of IT Communication Channels	0.160**	0.08	−0.18**	−0.05	−0.02	−0.02	0.124**	0.226**	−0.14**	0.243**	1								
Perceived Org. Capability	−0.07	−0.08	−0.03	0.01	0.04	−0.03	−0.01	0.01	−0.18**	0.305**	0.124**	1							
Ln.Full-Time Employees	−0.01	0.110*	−0.14**	0	0.096*	−0.01	0.102*	0.366**	−0.12**	0.122**	0.241**	0.086*	1						
City Manager Department	0.09	0.05	−0.05	0.01	0.01	−0.04	−0.01	−0.002	0.02	0.106*	0.184**	0.122**	0.03	1					
Community Development Department	−0.03	−0.04	0.02	−0.01	−0.03	−0.01	−0.03	−0.05	−0.02	−0.08	−0.08	−0.097*	−0.29**	−0.24**	1				
Finance Department	0.116*	−0.02	0.02	−0.01	0.03	0.04	−0.01	0.07	0.120**	−0.13**	−0.26**	0.06	−0.22**	−0.22**	−0.27**	1			
Parks Department	−0.01	−0.08	−0.03	0.04	−0.05	0.03	0.04	0.01	−0.08	0.002	0.109**	−0.14**	0.01	−0.22**	−0.27**	−0.25**	1		
Police Department	−0.16**	0.086*	0.03	−0.04	0.05	−0.03	0.01	−0.02	−0.04	0.105*	0.06	0.07	0.463**	−0.23**	−0.28**	−0.26**	−0.26**	1	
Years of Experience in the Private Sector	0.06	−0.08	0.04	−0.02	0.05	0.04	−0.004	−0.004	0.08	−0.07	−0.19**	−0.01	−0.13**	−0.08	0	0.257**	−0.088*	−0.093*	1

** Correlation is significant at the 0.01 level (2-tailed)
* Correlation is significant at the 0.05 level (2-tailed).

Table 3
Logistic regression models predicting security breaches and unauthorized data disclosures.

	Security Breaches			Unauthorized Data Disclosures		
Parameter	β	AME	Std. Error	β	AME	Std. Error
Organizational Factors						
Centralization	−0.056	−0.014	0.182	0.073	0.005	0.292
Risk-Taking	−0.121	−0.030	0.176	−0.384	−0.028	0.276
Number of IT Communication Channels	0.218***	0.054	0.062	0.161*	0.012	0.093
IT Capacity	−0.309**	−0.077	0.141	−0.446**	−0.033	0.222
Environmental Determinants						
Council-Manager	−0.670**	−0.160	0.296	0.135	0.010	0.407
# Partisan Shifts in the last 10 elections (ln)	−0.488*	−0.121	0.292	0.494	0.037	0.441
Margin of Partisan Vote	−0.438	−0.108	1.422	3.221*	0.238	1.912
Gini Coefficient	1.198	0.297	4.052	7.515	0.556	6.482
Lieberson Index of Inequality	−1.152	−0.286	0.943	−1.126	−0.083	1.350
Population (2017) (ln)	0.302	0.075	0.194	0.326	0.024	0.320
Control Variables						
Mayor's office	1.017***	0.248	0.377	−0.115	−0.008	0.483
Community Development Department	0.671*	0.166	0.404	−0.620	−0.040	0.564
Finance Department	1.619***	0.378	0.405	−0.114	−0.008	0.639
Parks Department	0.688*	0.170	0.383	−1.353**	−0.074	0.609
Full-Time Employees (ln)	0.008	0.002	0.088	0.085	0.006	0.137
Years of Experience in the Private Sector	0.025	0.006	0.019	−0.053*	−0.004	0.028
Intercept	−3.390		2.746	−6.960		4.683
Nagelkerke R Square	0.177			0.148		
N	393			468		

AME: Average Marginal Effects
Unstandardized Coefficients, Reference Category: Police Department.
* $p < 0.1$,
** $p < 0.05$,
*** $p < 0.01$

occurrence of cybercrime in local city government settings. Future studies should try to understand the reasons behind these opposite results and the extent to which the different nature of the phenomena studied may contribute determining these findings. A possible justification has been provided by Besley, Persson, and Sturm (2010) who suggest that higher levels of political competition at the state level could benefit citizens because politicians are incentivized to appeal to voters by putting in place policies that can increase their well-being, reducing dissatisfactions and motivations to commit cyberattacks. Conversely, nationwide political events and conflicts may be more ideological, motivating offenders to target departments deemed to not align with their beliefs.

Our findings have three main implications for cyber-incidents public organizations. First, cyber-incidents in government are primarily an organizational phenomenon. Our results confirm that accessible targets lacking capable guardians will experience cyber-incidents (e.g. crime). We extend RAT's validity to public organizations, by showing that organizational complexity plays a role in predicting cyber-incidents (Conklin & White, 2006). To prevent cyber-incidents, public organizations should invest to develop technological, and social forms of guardianship (Holt & Bossler, 2016). To this extent, research finds that cybersecurity exercises and cyber-risk assessments enhance public agencies' preparedness and increase organizations' ability to detect, face, and respond to cyberattacks, minimizing the damages stemming from them (Conklin & White, 2006). Moreover, literature recommends public agencies to develop effective inter-organizational collaborations which could provide small organizations with sufficient resources and IT capacities to face and counter cyber threats (Atkins & Lawson, 2020).

Second, in a challenge to previous research (Yar, 2005), our findings suggest that the ecological environmental elements of RAT (i.e. the time and space where crimes take place) play a role with regards to some specific types of cyber-incidents. We find that the level of political competition and the form of government are significantly associated with security cyber-incidents breaches in city departments. Practitioners who aim to minimize cyber-incidents risks should carefully assess both the political and the administrative contexts in which their organizations operate.

Third, by extending RAT to the public sector cyberworld, our results indicate that public managers who want to prevent cyber-incidents, should carefully consider and assess the value, visibility, and accessibility of their departments as targets. Public managers and organizations need to developpolicies that best fit the organizational features and weaknesses that are significantly related to cyber-incidents.

6. Conclusion

Cyber-incidents targeting cities represent serious threats to cities. Public managers in city departments are increasingly required to take actions to prevent these events from occurring or to promptly and effectively respond to them.

We apply RAT to investigate the determinants of cyber-incidents among US city departments. Our framework postulates that cyber-incident determinants might be both environmental and organizational. Our results show that some environmental aspects play a role in influencing the likelihood of experiencing cyber-incidents, while organizational aspects, such as points of access and IT capacity, predict security breaches and unauthorized data disclosures.

This study contributes to the cybercrime literature in several ways. First, we study cyber-incidents in a context usually overlooked: the public sector (Norris et al., 2019). Second, we investigate organizations rather than individuals as targets of cyber-incidents. We apply RAT to public organizations and find that both organizational and political aspects in the environment are related to cyber-incidents. Third, we adapt the environmental context from RAT to the cyberworld, demonstrating that it can help explain the likelihood of incurring security breaches in city departments.

Future studies should assess not only the occurrence of cyber-incidents in government but also their outcomes. Moreover, questions on how to effectively balance accessibility and cybersecurity needs of public organizations deserve greater attention. Finally, studies including both offenders and targets would provide a more complete picture of the causes of these threatening phenomena.

Funding

This work was supported by funding from Center for Science, Technology and Environmental Policy Studies (C-STEPS) at ASU.

Author statement

Mattia Caldarulo: Study conceptualization, Study methodology, Data analysis, Data interpretation, Paper drafting, Paper review and editing.

Eric W. Welch: Study conceptualization, Study methodology, Data collection, Data interpretation, Paper review and editing.

Mary K. Feeney: Study conceptualization, Study methodology, Data collection, Data interpretation, Paper review and editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Alternative models

Table A1
Alternative model - I Don't Know Coded as No.

	Security Breaches		Unauthorized Data Disclosures	
Parameter	β	Std. Error	β	Std. Error
Organizational Determinants				
Centralization	−0.003	0.169	0.085	0.299
Risk-Taking	0.037	0.154	−0.363	0.271
Number of IT Communication Channels	0.145***	0.053	0.140	0.093
IT Capacity	−0.136	0.126	−0.358*	0.206
Environmental Determinants				
Council-Manager	−0.624**	0.258	0.206	0.402
# Partisan Shifts in the Last 10 (ln)	−0.515**	0.259	0.428	0.416
Margin of Partisan Vote	−0.469	1.266	3.139*	1.809
Gini Coefficient	1.196	3.757	5.996	6.182
Lieberson Index of Inequality	−1.216	0.852	−0.836	1.246
Ln.Population (2017)	0.143	0.172	0.241	0.314
Control Variables				
City Manager Department	1.153***	0.350	−0.095	0.465
Finance Department	1.348***	0.372	−0.439	0.627
Parks Department	0.427	0.355	−1.473**	0.606
Community Development Department	0.377	0.365	−0.682	0.553
Ln.Full-Time Employees	0.051	0.081	0.074	0.129
Years of Experience in the Private Sector	0.025	0.017	−0.050*	0.029
Intercept	−2.875	2.388	−5.661	4.530
Nagelkerke R Square	0.137		0.133	
N	507		507	

Unstandardized Coefficients, Reference Category: Police Department.
* $p < 0.1$,
** $p < 0.05$,
*** $p < 0.01$

References

Alesina, A., Piccolo, S., & Pinotti, P. (2019). Organized crime, violence, and politics. *Review of Economic Studies, 86*(2), 457–499.

Andrews, R., Boyne, G. A., Law, J., & Walker, R. M. (2009). Centralization, organizational strategy, and public service performance. *Journal of Public Administration Research and Theory, 1*(1), 57–80.

Atkins, S., & Lawson, C. (2020). An improvised patchwork: Success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review, 81*(5), 847–861. https://doi.org/10.1111/puar.13322

Beavon, D. J. K., Brantingham, P. L., & Brantingham, P. J. (1994). The influence of street networks on the patterning of property offenses. *Crime Prevention Studies, 2*, 115–148.

Besley, T., Persson, T., & Sturm, D. M. (2010). Political competition, policy and growth: Theory and evidence from the US. *The Review of Economic Studies, 77*(4), 1329–1352.

Bourgon, J. (2009). New directions in public administration serving beyond the predictable. *Public Policy and Administration, 24*(3), 309–330. https://doi.org/10.1177/0952076709103813

Brewster, B., Kemp, B., Galehbakhtiari, S., & Akhgar, B. (2015). Cybercrime: Attack motivations and implications for big data and National Security. In B. Akhgar, G. B. Saathoff, H. R. Arabnia, R. Hill, A. Staniforth, & P. S. Bayerl (Eds.), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies* (pp. 108–127).

Carr, J. B. (2015). What have we learned about the performance of council-manager government? A review and synthesis of the research. *Public Administration Review, 75*(5), 673–689. https://doi.org/10.1111/puar.12415

Caruson, K., Macmanus, S. A., & McPhee, B. D. (2012). Cybersecurity policy making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success. *Homeland Security & Emergency Management, 9*(2), 1–22. https://doi.org/10.1515/jhsem-2012-0003

Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308–333.
Coccia, M. (2017). A theory of general causes of violent crime: Homicides, income inequality and deficiencies of the heat hypothesis and of the model of CLASH. *Aggression and Violent Behavior, 37*, 190–200.
Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.
Conklin, A., & White, G. B. (2006). E-government and cyber Security: The role of cyber Security exercises. In *Proceedings of the 39th Hawaii International Conference on System Sciences*.
Desai, V. M. (2008). Constrained growth: How experience, legitimacy, and age influence risk taking in organizations. *Organization Science, 19*(4), 594–608. https://doi.org/10.1287/orsc.1070.0335
DHS. (2019). Cyber incident reporting: A unified message for reporting to the Federal Government. https://www.dhs.gov/sites/default/files/publications/CyberIncident Reporting United Message.pdf.
Feeney, M., & Brown, A. (2017). Are small cities online? Content, ranking, and variation of US municipal websites. *Government Information Quarterly, 34*(1), 62–74.
Feeney, M., Fusi, F., Camarena, L., & Zhang, F. (2019). Towards more digital cities? Change in technology use and perceptions across small and medium-sized US cities. *Local Government Studies, 46*(5). https://doi.org/10.1080/03003930.2019.1690993
Fricker, S., Galesic, M., Tourangeau, R., & Yan, T. (2005). An experimental comparison of web and telephone surveys. *Public Opinion Quarterly, 69*(3), 370–392. https://doi.org/10.1093/poq/nfi027
Funk, K., Martin, C., DuPuis, N., Shark, A., & Bowen, D. (2019). *Protecting our data: What cities should know about cybersecurity*.
Fusi, F., & Feeney, M. (2018). Electronic monitoring in public organizations: Evidence from US local governments. *Public Management Review, 20*(10), 1465–1489. https://doi.org/10.1080/14719037.2017.1400584
Fusi, F., & Feeney, M. (2020). Data sharing in small and medium US cities: The role of community characteristics. *Public Administration, 98*(4), 922–940. https://doi.org/10.1111/padm.12666
Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Social, political, economic and cultural. *IEEE Technology and Society Magazine, 30*(1), 28–38.
GAO. (2016). *Agencies Need to Improve Controls over Selected High-Impact Systems*.
Graham, R. (2020). Race, social media, and deviance. In T. J. Holt, & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and Cyberdeviance* (1st ed., pp. 67–90). Palgrave Macmillan.
Graham, R., & Triplett, R. (2017). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior, 38*(12), 1371–1382. https://doi.org/10.1080/01639625.2016.1254980
Handlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider. In J. McAlaney, L. A. Frumkin, & V. Benson (Eds.), *Psychological and behavioral Examinations in Cyber Security*. IGI Global.
Hannan, M. T., & Freeman, J. (1984). Structural inertia and organizational change. *American Sociological Review, 49*(2), 149–164.
Hipp, J. R. (2007). Income inequality, race and place: Does the distribution of race and class within neighborhoods affect crime rates? *Criminology, 45*(3), 665–697.
Holt, T. J., & Bossler, A. M. (2016). Applications of criminological theory to cybercrimes. In *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge.
Holt, T. J., Leukfeldt, R., & Van De Weijer, S. (2020). An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites. *Criminal Justice and Behavior, 47*(4), 487–505. https://doi.org/10.1177/0093854819900322
IBM Security. (2020). *Cost of a Data Breach Report 2019*.
Ife, C. C., Davies, T., Murdoch, S. J., & Stringhini, G. (2019). Bridging information Security and environmental criminology research to better mitigate cybercrime. *ArXiv*.
Isett, K. R., Mergel, I. A., LeRoux, K., Mischen, P. A., & Rethemeyer, R. K. (2011). Networks in public administration scholarship: Understanding where we are and where we need to go. *Journal of Public Administration Research and Theory, 21*(suppl_1), i157–i173.
Jahankhani, H., Al-Nemrat, A., & Hosseinnian-Far, A. (2014). Cybercrime classification and characteristics. In B. Akhgar, A. Staniforth, & F. Bosco (Eds.), *Cyber crime and cyber terrorism Investigator's handbook* (1st ed., pp. 149–164). Syngress.
Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology, 10*(1), 79–91. https://doi.org/10.5281/zenodo.58523
Kennedy, B. P., Kawachi, I., Prothrow-Stith, D., Lochner, K., & Gupta, V. (1998). Social capital, income inequality, and firearm violent crime. *Social Science & Medicine, 47*(1), 7–17.
Lawrence, P. R., & Lorsch, J. W. (1967). Differentiation and integration in complex organizations. *Administrative Science Quarterly, 12*(1), 1–47.
Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280.
Lieberson, S. (1969). Measuring population diversity. *American Sociological Review, 34*(6), 850–862.
Lincoln, J. R., & Zeitz, G. (1980). Organizational properties from aggregate data: Separating individual and structural effects. *American Sociological Review, 45*(3), 391–408.
Lindblom, C. E. (1959). The Science of "Muddling Through". *Public Administration Review, 19*(2), 79–88.
Macmanus, S. A., Caruson, K., & McPhee, B. D. (2013). Cybersecurity at the local government level: Balancing demands for transparency and privacy rights. *Journal of Urban Affairs, 35*(4), 451–470.
Maume, D. J. (1989). Inequality and metropolitan rape rates: A routine activity approach. *Justice Quarterly, 6*(4), 513–527. https://doi.org/10.1080/07418828900090361
McCaghy, C. H., Capron, T. A., Jamieson, J. D., & Carey, S. H. (2008). *Deviant behavior: Crime, conflict and interest groups* (8th ed.) Routledge.
Metz, N., & Burdina, M. (2018). Neighbourhood income inequality and property crime. *Urban Studies, 55*(1), 133–150.
Mikalef, P., van de Wetering, R., & Krogstie, J. (2021). Building dynamic capabilities by leveraging big data analytics: The role of organizational inertia. *Information & Management, 58*. https://doi.org/10.1016/j.im.2020.103412
Moon, M. J. (1999). The pursuit of managerial entrepreneurship: Does organization matter? *Public Administration Review, 59*(1), 31–43.
Moon, M. J., & Bretschneider, S. I. (2002). Does the perception of red tape constrain IT innovativeness in organizations? Unexpected results from a simultaneous equation model and implications. *Journal of Public Administration Research and Theory, 12*(2), 273–291.
Mossberger, K., Wu, Y., & Crawford, J. (2013). Connecting citizens and local governments? Social media and interactivity in major U.S. Cities. *Government Information Quarterly, 30*, 351–358. https://doi.org/10.1016/j.giq.2013.05.016
Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793.
Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. *Public Administration Review, 79*(6), 895–904.
O'Brien, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality & Quantity, 41*, 673–690.
Ochsner, K. (2000). Are affective events richly recollected or simply familiar? The experience and process of recognizing feelings past. *Journal of Experimental Psychology: General, 129*, 242–261.
Olzak, S. (1990). The political context of competition: Lynching and urban racial violence, 1882–1914. *Social Forces, 69*(2), 395–421.
Ousey, G. C., & Lee, M. R. (2013). Community, inequality, and crime. In F. T. Cullen (Ed.), *The Oxford handbook of criminological theory*. Oxford University Press.
Park, J., Cho, D., Lee, J. K., & Lee, B. (2019). The economics of cybercrime: The role of broadband and socioeconomic status. *ACM Transactions on Management Information Systems, 10*(4).
Pfeffer, J., & Salancik, G. R. (1978). Social control of organizations. In *The external control of organizations: A resource dependence perspective* (pp. 39–60). Harper & Row.
Preis, B., & Susskind, L. (2020). Municipal cybersecurity: More work needs to be done. *Urban Affairs Review, 1–16*. https://doi.org/10.1177/1078087420973760
Rainey, H. G. (2009). *Understanding and managing public organizations* (4th ed.). Jossey-Bass.
Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior, 38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448
Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135.
Ropek, L. (2020). *Anonymous claims responsibility for Minneapolis PD Cyberattack*. Government Technology. https://www.govtech.com/security/Anonymous-Claims-Responsibility-for-Minneapolis-PD-Cyberattack.html.
Scott, W. R., & Davis, G. F. (2007). *Organizations and organizing: Rational, natural and open system perspectives*. Routledge.
Shively, J. (2021). Cybersecurity policy and the trump administration. *Policy Studies, 42*(5–6), 738–754. https://doi.org/10.1080/01442872.2021.1947482
Svaleryd, H., & Vlachos, J. (2009). Political rents in a non-corrupt democracy. *Journal of Public Economics, 93*(3–4), 355–372.
Terry, L. D. (1998). Administrative leadership, neo-managerialism, and the public management movement. *Public Administration Review, 58*(3), 194–200.
The Economist. (2017, May). *The World's Most Valuable Resource is No Longer Oil, but Data*. The Economist. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
Thompson, N., Mullins, A., & Chongsutakawewong, T. (2020). Does high e-government adoption assure stronger Security? Results from a cross-country analysis of Australia and Thailand. *Government Information Quarterly, 37*(1). https://doi.org/10.1016/j.giq.2019.101408
Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government Information Quarterly, 32*(3), 316–322. https://doi.org/10.1016/j.giq.2015.05.001
Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly, 28*(2), 164–175. https://doi.org/10.1016/j.giq.2010.06.008
Yar, M. (2005). The Novelty of "Cybercrime". *European Journal of Criminology, 2*(4), 407–427.
Zhang, F., & Feeney, M. (2020). Engaging through technology: The role of administrative culture and mandates. *Public Management Review, 22*(10), 1423–1442. https://doi.org/10.1080/14719037.2019.1630475

Mattia Caldarulo is a PhD student in Public Administration and Public Policy at the School of Public Affairs at Arizona State University. Caldarulo works as a Graduate Research Assistant at the Center for Science, Technology, and Environmental Policy

Studies (C-STEPS). His research focuses on risk management in public agencies, technology in government, and science policy.

Eric W. Welch is a professor in the School of Public Affairs at Arizona State University where he teaches decision making, organization and network theory, institutional design, and science and innovation policy. His primary research interests include organizational adaptation to climate change, science policy, and digital government. Dr. Welch currently directs the Center for Science, Technology and Environmental Policy Studies (C-STEPS) at ASU. He is an affiliated faculty member in the ASU School for the Future of Innovation and Society and in the Center for Organization Research and Design, as well as senior sustainability scientist in the ASU Julie Ann Wrigley Global Institute of Sustainability.

Mary Feeney is professor and Lincoln Professor of Ethics in Public Affairs at Arizona State University. Her research focuses on technology in government, science and technology policy, and public and nonprofit management. Dr Feeney is a Fellow of the National Academy of Public Administration.