The economic drivers of cyber risk

Galen Sher*

March 2026

Abstract

I compile new data across US states to show that cyberattacks become more frequent after increases in unemployment, output, digitalization, and inequality. Law enforcement, in the form of employing more public cybersecurity workers, is effective at deterring cyberattacks. These findings support the economic theory of crime applied to the cyber domain, in which crime depends on motivation and opportunity. They also support the social disorganization and strain theories of crime. Furthermore, I show that the severity of the associated cyberattack losses increases with output, suggesting that higher output provides more opportunity for theft, damage, or disruption. Both the frequency and the severity of cyberattacks depend more on national economic conditions than on local conditions. I develop a simple general equilibrium model of cybercrime that rationalizes these findings and links the literature on cyber risk to the literature on the economics of crime. These findings suggest that cyber risk contains an aggregate component that is not diversifiable within an economy.

JEL: K42, E32, L86
Keywords: cyberattack; cybercrime; cyber risk; cybersecurity; economics of crime; digitalization

1 Introduction

Cyberattacks have become a quantitatively important feature of modern economies.[1] The median estimate surveyed in Cobos et al. (2024) puts

*International Monteary Fund. The views expressed are those of the author and do not reflect those of the IMF, its management, or executive board.

[1]The National Institute for Standards and Technology defines a cyberattack as any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

the global economic losses at around 0.6 percent of global GDP annually. Official estimates of national losses are between 0.3 and 0.6 percent in the United States in 2016 and 1.3 percent in the UK in 2011 (Council of Economic Advisers 2018; Cobos et al. 2024). These are direct costs including financial losses and damages, but the indirect costs from business disruption, reputational damage, and spillovers to other firms are orders of magnitude larger (Kamiya et al. 2021; Crosignani, Macchiavelli, and Silva 2023). Even the risk of potential cyberattacks has led to rapid growth of the cybersecurity industry, which could account for around 0.2 percent of GDP in the US.[2] Policymakers view cyberattacks as a risk to financial stability, especially if these were to target critical infrastructures like payment systems or cloud computing providers (Office of Financial Research 2017; International Monetary Fund 2024). Disruptions to critical infrastructure, like attacks that have already occurred on oil pipelines (e.g., 2021 Colonial Pipeline incident in the US) and power grids (e.g., 2015 power grid hack in Ukraine), could also affect economic activity.

The literature has focused on the drivers of cyber risk at the firm level, finding that larger firms, firms in the financial sector, and firms with more intangible assets are more likely to be targeted (Aldasoro et al. 2022; Jamilov, Rey, and Tahoun 2021). Other research highlights market failures in cybersecurity provision—arising from misaligned incentives, information asymmetries, and network externalities—that lead to underinvestment in protection (Anderson and Moore 2006). Still other studies have examined the drivers of operational risk, which is a broader concept than cyber risk,[3] finding that losses from operational risk in the financial sector increase after deterioration in the macroeconomic environment, credit booms, and periods of excessively accommodative monetary policy (Abdymomunov, Curti, and Mihov 2020; Aldasoro et al. 2020).

Theory predicts that economic conditions should drive cyberattacks. If cyberattacks are viewed as a type of property crime, then the Becker–Erlich theory predicts that they should be described by motivation and opportunity—bad economic conditions should motivate more people to engage in cyberattacks, while high levels of output and little law enforcement should provide more opportunity for cyberattacks. Increases in inequality could also weaken informal social controls on crime (known as social disorganization theory) and lead to dissatisfaction that encourages more people to engage in crime (strain theory) (Kelly 2000). Little is known, however,

[2]Based on industry estimates of revenues of US$ 68 billion in 2023 and a share of value added in output of 70 percent from the Bureau of Economic Analysis' digital economy satellite accounts.

[3]Operational risk includes the risk to business processes, not just information systems, from events including errors, fraud, misconduct, system failures, and poor decisions, not just from cyberattacks.

about whether these economic conditions drive cyber risk over time.

This paper fills that gap. I provide the first systematic empirical analysis of the relationship between macroeconomic conditions and cyber risk, covering both the frequency and the severity of cyberattacks. Using newly compiled data across US states since 2001, based on complaints received by the FBI's Internet Crime Complaint Center, I examine how cyberattacks respond to changes in unemployment, output, digitalization, inequality, poverty, and public resources devoted to cybersecurity. The analysis combines national-level time series evidence with state-level panel variation and applies a range of estimators including least squares, fixed effects, instrumental variables, and generalized method of moments (GMM).

The paper makes four contributions to the literature.

First, it finds evidence to support the motivation and opportunity theories as driving cyberattacks. Cyberattacks become more frequent following increases in unemployment, reflecting higher motivation, and after increases in real GDP per person, reflecting more opportunity for theft, damage, or disruption. Law enforcement also deters cyberattacks, with attacks becoming less frequent after more federal cybersecurity workers are employed. One key distinction from the Becker–Ehrlich model is that cybercrime takes place remotely, which shows up in the analysis—national economic conditions dominate local conditions in driving cyberattacks. The cyclicality of cyberattacks means that cyber risk contains an aggregate component that is not diversifiable within an economy, with implications for economic dynamics, public spending on cybersecurity, stabilization policy, and insurance markets.

Second, the paper finds that the severity of cyberattacks, that is, the losses from the average attack, are increasing in real GDP per person. This extends the standard Becker–Ehrlich model loss (damage) function, which depends only on probability of being targeted.

Third, the paper finds evidence that inequality drives cyberattacks, which supports the social disorganization and strain theories.

Fourth, the paper rationalizes the empirical findings by developing a simple general equilibrium model of production, labor supply, and cybercrime. Building on the economics of crime framework of Becker (1968), Ehrlich (1973), Furlong (1987), and Sah (1991), the model embeds cybercrime into an economy with digital capital and law enforcement. Calibrating the model to the US, comparative statics show that higher unemployment encourages people to shift from formal work into cybercrime, tougher punishment (including higher probabilities of being caught) deters cybercrime, and digitalization increases opportunities for cybercrime.

The remainder of the paper is structured as follows. Section 2 presents national-level evidence on cyberattacks and macroeconomic conditions. Section 3 exploits state-level variation and estimates dynamic panel models

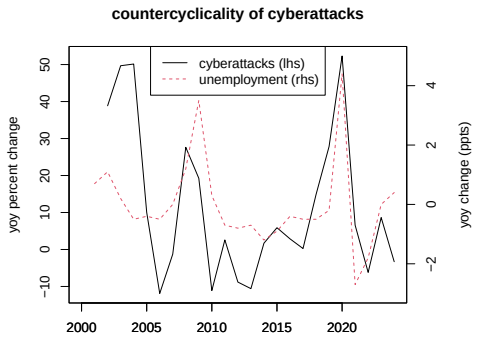


Figure 1: The solid black line shows the growth in the rate of cyberattacks per hundred thousand people in the United States, based on complaints received by the FBI's Internet Crime Complaint Center. The dashed red line shows the year-to-year change in the US unemployment rate.

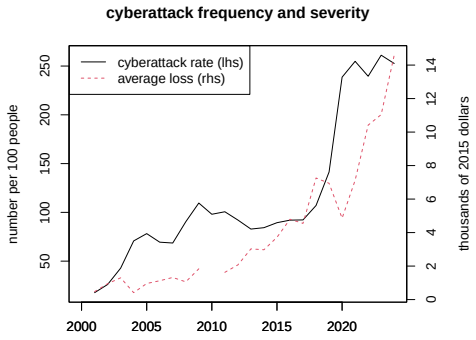


Figure 2: The solid black line shows the evolution over time in the number of cyberattacks each year per hundred thousand people in the United States. The dashed red line shows the size of the average real loss per cyberattack, in thousands of 2015 US dollars. These figures are based on complaints received by the FBI's Internet Crime Complaint Center. The datapoint for losses in 2010 is not available.

of cyberattack frequency and severity. Section 4 develops the theoretical model and links it to the empirical results. Section 5 concludes and draws out implications for research and policy.

2 National-level evidence

We begin by examining evidence for the simplest possible relationship—a relationship over time between all cyberattacks in the United States and US economic conditions. Figure 1 motivates this analysis with suggestive graphical evidence that cyberattacks become more frequent during increases in unemployment, with spikes occurring around the global financial crisis and COVID-19 pandemic.

Letting y_t denote the natural logarithm of the number of cyberattacks nationally per hundred thousand people in year t,[4] I model the growth in

[4]All data sources and variable definitions are provided in Appendix B.

the number of cyberattacks per hundred thousand people as

$$\Delta y_t = \gamma + \sum_{k}^{p} \alpha_k \Delta y_{t-k} + x_t'\beta + u_t. \tag{1}$$

The vector x_t represents US economic conditions, including the change in the unemployment rate, the growth rate of real GDP per person, and the growth in the number of internet users as a measure of digitalization. This model allows the growth in the number of cyberattacks to depend on up to four prior years of its own values, which turns out to be adequate to account for heteroskedasticity in the error term u_t. The model is specified in growth rates (Δy_t) rather than levels (y_t) to avoid potential nonstationarity, given that y_t trends upward over time (Figure 2). The parameters to be estimated are the scalars $\gamma, \alpha_1, \ldots, \alpha_k$ and the vector β.[5]

Columns (1) and (2) of Table 1 show the results of estimating the parameters in equation (1) by least squares. Given the small sample of 19 observations, the standard errors in parentheses in Columns (1)-(2) assume homoskedastic and normally distributed errors u_t, which are not rejected by the Breusch-Pagan and Shapiro-Wilk tests in Column (1).[6] $p = 4$ lags turn out to be enough to account for heteroskedasticity. Column (1) suggests a countercyclical pattern where higher unemployment leads to more cyberattacks in the country, after controlling for typical dynamics in cyberattacks over time. A one percentage point increase in the unemployment rate is associated with a 6.2 percent increase in the number of cyberattacks per person in the short run, and a 6.5 percent ($= 6.273/(1-\hat{\alpha}_1-\hat{\alpha}_2-\hat{\alpha}_3-\hat{\alpha}_4)$) increase in the long run. Similarly, decreases in real GDP per person lead to more cyberattacks in Column (2), with a 1 percent reduction in real GDP per person leading to a 4.8 percent increase in the number of cyberattacks per person in the short run, and 4.9 percent in the long run. These cyclical patterns of cyberattacks are consistent with the motivation theory of crime, where higher unemployment drives more people into becoming malicious cyber actors, as in models where individuals choose rationally between work and crime (Furlong 1987; Sah 1991). When both unemployment and real GDP per person are included at the same time, Column (3) shows that the estimated coefficient on real GDP per person becomes positive, suggesting some support also for the opportunity theory of crime. These coefficients are not statistically significant, but state-level evidence in the next section will be able to identify them.

Beyond these macroeconomic relationships, directing public resources to cybersecurity also seems to reduce the frequency of cyberattacks. Col-

[5] Δ denotes the year-to-year change (e.g., $\Delta y_t = y_t - y_{t-1}$) and $'$ denotes the transpose.

[6] In Appendix A, I show that the statistical significance of the estimates is similar if we assume that the sample size is large enough to appeal to asymptotic heteroskedasticity- and autocorrelation-consistent standard errors.

umn (4) shows that the number of federal workers employed at the Cybersecurity and Infrastructure Security Agency (CISA) and its predecessor (the National Protection and Programs Directorate (NPPD)) is negatively related to the number of cyberattacks. A one percent increase in the number of federal cybersecurity workers, after controlling for two lags and the unemployment rate, leads to a 0.4 percent reduction in the number of cyberattacks per person in the short run, which persists at 0.3 percent ($= -0.35/(1 - \hat{\alpha}_1 - \hat{\alpha}_2)$ in the long run. Given potential reverse causality from cyberattacks to public investment in cybersecurity, Column (4) instruments the number of cybersecurity workers by two lags in the numbers of Republicans and Democrats in the House of Representatives, and two lags in the year-to-year changes in the numbers of Republicans and Democrats.[7] The Olea and Pflueger (2013) effective F statistic in the first stage does not reject the hypothesis that the instruments are informative enough to contain the bias within a fraction $\tau = 0.3$ of the worst case benchmark.

This section showed evidence of a relationship between economic conditions and the *frequency* of cyberattacks. However, similar models at the national level did not produce evidence of any relationship with the *severity* of cyberattacks, i.e., real losses on the average cyberattack. This lack of evidence might be driven by the small sample size at the national level, because subsequent sections do find such evidence at the state level.

3 Evidence from US states

State-level evidence gives a larger sample size, which allows us to test for the importance of digitalization, poverty, and inequality, and allows to compare the relative effects of local economic conditions (at the state level) to national conditions.

3.1 Fixed effects estimation

3.1.1 Fixed effects estimation of the frequency of cyberattacks

If we denote by y_{it} the natural logarithm of the number of cyberattacks per hundred thousand people in state i and year t, then I specify the model as

$$\Delta y_{i,t} = \sum_{k=1}^{p} \alpha_k \Delta y_{i,t-k} + x_t'\beta + x_{i,t}'\delta + c_i + v_{i,t} \tag{2}$$

[7] Column (4) therefore uses asymptotic standard errors. Fewer lags ($p = 2$) of the dependent variable are necessary as controls in this case because there is no need to ensure homoskedasticity of the residuals, the sample size is small, and the coefficients on the third and fourth lags are not statistically significant.

Table 1: National-level frequency of cyberattacks and macroeconomic activity

	(1)	(2)	(3)	(4)
$L(\Delta y_{i,t})$	0.340	0.559**	0.305	−0.039
	(0.221)	(0.232)	(0.297)	(0.222)
$L^2(\Delta y_{i,t})$	−0.352	−0.444*	−0.337	−0.011
	(0.220)	(0.234)	(0.242)	(0.151)
$L^3(\Delta y_{i,t})$	0.265	0.328	0.249	
	(0.232)	(0.255)	(0.256)	
$L^4(\Delta y_{i,t})$	−0.219	−0.210	−0.216	
	(0.182)	(0.195)	(0.190)	
ΔUS unemp$_t$	6.273***		7.245	8.083***
	(1.977)		(5.513)	(1.345)
$\Delta \log$(US rgdppc)$_t$		−4.750***	0.876	
		(1.767)	(4.614)	
$\Delta \log$(CISA pp)$_t$				−0.350**
				(0.142)
Constant	0.072*	0.113**	0.064	0.102***
	(0.040)	(0.047)	(0.059)	(0.028)
Method:	OLS	OLS	OLS	2SLS
Breusch-Pagan p-value:	0.3709	0.0719	0.5926	
Shapiro-Wilk p-value:	0.7061	0.3403	0.8789	
Observations	19	19	19	18
R^2	0.582	0.524	0.583	0.687
Note:				*p<0.1; **p<0.05; ***p<0.01

where x_t is a vector containing national economic conditions, specifically the change in the US unemployment rate, the growth rate of US GDP per person, the growth rate of the number of internet users in the US, the change in the poverty rate, and the change in the Gini coefficient of income inequality. The vector $x_{i,t}$ contains the change in state-level economic conditions: the unemployment rate and the growth rate of Gross State Product (GSP) in state i. The error terms $c_i, v_{i,t}$ are thought of as random variables that capture unobservables. The parameters to be estimated are $\alpha_1, \ldots, \alpha_p, \beta$, and δ.

I begin with a canonical fixed effects estimation of (2). The fixed effects estimator assumes strict exogeneity, i.e. $E(v_{i,t}|\ldots, c_i) = 0$ where $\ldots$ denotes all lags and leads of the variables on the right-hand side of equation (2). If $\alpha_k \neq 0$, then strict exogeneity will not hold and the fixed effects estimator will be biased (Nickell 1981), although this bias vanishes as T gets large. The bias may not be substantive in our setting, given Monte Carlo evidence in Judson and Owen (1999) showing that the bias on the coefficients β and δ is only around 1 percent with $p = 1$, $\alpha_1 = 0.2$, and $T = 20$, which is close to our sample size. Nevertheless, in the subsequent section, I use a Generalized Methods of Moments (GMM) estimator to avoid this bias.

Column (1) of Table 2 shows the results of estimating specification (2) for unemployment and production at the national and state levels, with standard errors that allow for spatial and temporal dependence shown in parentheses (following Driscoll and Kraay (1998)). The estimations use a lag length of $p = 2$, which is the lag length selected by the GMM estimator in the subsequent section.[8] With both unemployment and real GDP per person included in Column (1), the coefficients on both become positive, matching the pattern in Column (3) of Table 1. Again, the positive coefficient on unemployment is consistent with the motivation theory and that on real GDP per person is consistent with the opportunity theory.

Both national and state-level economic conditions have statistically significant effects on cyberattacks in Column (1). National unemployment, for example, seems to motivate cyberattacks across all states, and even holding national unemployment constant, state-level unemployment further motivates cyberattacks. Coefficients on national level unemployment and real GDP per person are over seven times as large as those on state level variables, which could reflect the fact that cyberattacks happen remotely. For example, Internet Crime Complaint Center (2010) shows that most cyberattacks are committed across state lines. The state with the highest proportion of in-state perpetrators in 2010 was California, at 39

[8]Robustness checks in Appendix A reveal that the effects of national economic conditions, and to some extent those of state conditions, are robust to using longer lag lengths.

Table 2: State-level frequency of cyberattacks and macroeconomic activity, estimated by fixed effects

	(1)	(2)	(3)
$L(\Delta y_{i,t})$	-0.024	0.018	-0.272^{***}
	(0.122)	(0.118)	(0.055)
$L^2(\Delta y_{i,t})$	-0.024	-0.117	-0.240^{***}
	(0.106)	(0.125)	(0.059)
$L^3(\Delta y_{i,t})$			-0.143^{**}
			(0.058)
ΔUS unemp$_t$	12.761^{***}	21.841^{***}	
	(2.752)	(3.422)	
$\Delta \log$(US rgdppc)$_t$	6.171^{**}	10.584^{***}	
	(2.569)	(2.018)	
Δstate unemp$_{i,t}$	1.342^{**}	0.915	0.718^{*}
	(0.604)	(0.723)	(0.424)
$\Delta \log$(state rgdppc)$_{i,t}$	0.788^{**}	0.733^{*}	0.483^{**}
	(0.380)	(0.429)	(0.211)
$\Delta \log$(US internet user)$_t$		1.181^{***}	
		(0.413)	
ΔUS inequality$_t$		0.116^{**}	
		(0.046)	
ΔUS poverty$_t$		-0.047	
		(0.036)	
state FE:	yes	yes	yes
time FE:	no	no	yes
partial R-squared:	0.255	0.34	0.035
N	51	51	51
T	20	20	19
Observations	1,020	1,020	969

Note: *p<0.1; **p<0.05; ***p<0.01

Driscoll and Kraay (1998) standard errors shown in parentheses.

percent. In Column (1), a one percentage point increase in in national unemployment is associated with a 13 percent increase in cyberattacks across all states (in the short-run), while the same increase in a state's unemployment only increases cyberattacks in that state by some 1.3 percent. A one percent increase in national real GDP per person is associated with a 6 percent increase in the number of cyberattacks per person (in the short run), and holding national economic conditions constant, a one percent increase in state GSP per person is associated with a 0.8 percent increase in the number of cyberattacks per person.

When I add other variables in Column (2), I find that digitalization, measured as the number of internet users nationwide, is associated with more cyberattacks in the average state. A one percent increase in the number of users is associated with a 1.2 percent increase in the number of cyberattacks per person in the short run (1.1 percent in the long run). Furthermore, increases in inequality are associated with more cybercrime, and there is no statistically significant relationship between cybercrime and poverty. This finding suggests that it is *relative* deprivation that drives cybercrime, by increasing the perceived returns and reducing the opportunity costs, rather than *absolute* deprivation. The poor might lack the resources (skills, hardware, and internet connection) to engage in cybercrime, given that people with a comparative advantage in cybercrime tend to be educated and skilled (Moore, Clayton, and Anderson 2009).

To test the effects of national economic conditions, Columns (1) and (2) omit time fixed effects from the specification. If I include time fixed effects and drop national economic conditions, Column (3) shows that the coefficients on the state unemployment rate and real GSP per person remain positive and statistically significant, confirming that they are not proxying for any unobserved global factors.[9]

3.1.2 Fixed effects estimation of the severity of cyberattacks

Denote the natural logarithm of the loss from the average cyberattack in state i in year t, in 2015 constant-price US dollars, by l_{it}. Then I model the year-to-year growth rate of losses as

$$\Delta l_{i,t} = \sum_{k=1}^{p} \alpha_k \Delta l_{i,t-k} + x_t'\beta + x_{i,t}'\delta + c_i + v_{i,t}, \tag{3}$$

where again x_t is a vector containing national economic conditions, specifically the growth rate of US real GDP per person, the change in the US unemployment rate, and the growth rate of the number of internet users in

[9] A third lag of the dependent variable is statistically significant in this case, but not a fourth (see Appendix A).

Table 3: State-level severity of cyberattacks and macroeconomic activity, estimated by fixed effects

	(1)	(2)	(3)	(4)	(5)
$L(\Delta l_{i,t})$	-0.451^{***}	-0.467^{***}	-0.473^{***}	-0.474^{***}	-0.440^{***}
	(0.074)	(0.072)	(0.061)	(0.061)	(0.076)
$L^2(\Delta l_{i,t})$	-0.451^{***}	-0.418^{***}	-0.414^{***}	-0.415^{***}	-0.399^{***}
	(0.049)	(0.061)	(0.068)	(0.069)	(0.059)
$\Delta \log(\text{US rgdppc})_t$	6.393^{***}		-1.727	-2.342	
	(1.584)		(4.597)	(4.558)	
$\Delta \log(\text{state rgdppc})_{i,t}$				0.966	
				(0.794)	
$\Delta \text{US unemp}_t$		-7.691^{***}	-9.362^{*}	-10.787^{**}	-3.131^{***}
		(0.906)	(4.946)	(5.106)	(0.970)
$\Delta \text{state unemp}_{i,t}$				2.042	
				(1.978)	
$\Delta \log(\text{US internet user})_t$	-1.218^{***}	-1.762^{***}	-1.906^{***}	-1.866^{***}	-1.961^{***}
	(0.384)	(0.305)	(0.512)	(0.511)	(0.331)
$\Delta y_{i,t}$					-0.535^{***}
					(0.088)
$(\Delta y_{i,t})^2$					-0.167
					(0.230)
state FE:	yes	yes	yes	yes	yes
time FE:	no	no	no	no	no
partial R-squared:	0.395	0.412	0.412	0.413	0.443
N	51	51	51	51	51
T	10	10	10	10	10
Observations	510	510	510	510	510

Note: *p<0.1; **p<0.05; ***p<0.01
Driscoll and Kraay (1998) standard errors shown in parentheses.

the US The vector $x_{i,t}$ contains state-level economic conditions: the growth rate of real Gross State Product (GSP) in state i and the change in the unemployment rate in state i. The error terms $c_i, v_{i,t}$ are random variables that capture unobservables. The parameters to be estimated are $\alpha_1, \alpha_2, \beta$, and δ. Table 3 shows the results of estimating this model by fixed effects with Driscoll-Kraay standard errors. Again, I assume a lag length of $p = 2$, which is the lag length selected by the GMM estimator in the subsequent section.[10]

In Column (1), higher national real GDP per person leads to larger losses from the average cyberattack. As the economy produces more, there is more output to steal or disrupt through cyberattacks. A one percent increase in US real GDP per person is associated with a 6.4 percent increase in the real loss from an average cyberattack. A similarly positive relationship has been found at the firm level, with larger firms in the financial

[10]Results for $p = 3$ lags are similar.

sector being more exposed to cyberattacks (Eling and Jung 2022; Jamilov, Rey, and Tahoun 2021). Column (1) also shows that more internet users is associated with lower losses on the average cyberattack, suggesting that, as more people become internet users, each successive user seems to be less valuable to malicious cyber actors than the previous user, or each successive malicious cyber actor is less capable.

Column (2) shows that higher national unemployment leads to smaller losses from the average cyberattack. There are two potential explanations. The first is that higher unemployment reflects lower production, which thus reflects the same relationship as with real GDP per person in Column (1). This interpretation is supported by the evidence in Column (3), which shows that the coefficient on real GDP per person loses its statistical significance when real GDP per person and unemployment are jointly included in the specification. A second potential explanation for the negative coefficient on unemployment in Column (2) is that higher unemployment drives more people into becoming malicious cyber actors, in line with the evidence in Section 3.1.1 and the motivation theory of crime, and that each new malicious cyber actor is less capable than the previous one, which brings down the average loss per attack.

State level economic conditions are not clearly linked to the loss from an average cyberattack. The GSP per person and unemployment rate in a state are not statistically significantly linked to the loss in that state (Column (4)), after controlling for national economic conditions, loss dynamics, and structural unobserved differences between states.

The frequency of cyberattacks $y_{i,t}$ is important for explaining the loss from the average cyberattack $l_{i,t}$. Column (5) shows that $\Delta y_{i,t}$ enters the specification with a negative coefficient, suggesting that more cyberattacks result in lower average losses, as every successive attack produces a smaller loss than that of the previous attack. Furthermore, the coefficient on $(\Delta y_{i,t})^2$ is not statistically significant. These two coefficients suggest that the damage function in the Becker–Ehrlich framework, which describes social losses from crime as a function $D(O)$ of the number of criminal offenses O, is concave for cyber offenses. Specifically, if $D(O) = O \cdot l(O)$, where $l(O)$ is the average loss as a function of the number of offenses, then $D''(O) = 2l'(O) + Ol''(O)$, and Column (5) indicates that $l'(O) < 0$ and $l''(O) \approx 0$. I return to this result using the GMM estimator below.

3.2 GMM estimation

To guard against potential bias in the fixed effects estimator in this dynamic panel setting, I also apply the "system GMM" estimator of Holtz-Eakin, Newey, and Rosen (1988), Arellano and Bond (1991), Arellano and Bover (1995), and Blundell and Bond (1998). Specifically, I take specifications

(2) and (3) and assume that error terms have zero mean and are serially uncorrelated, $E(c_i), E(v_{it}), E(c_i v_{jt}), E(v_{is} v_{jt}) = 0$, that initial conditions are predetermined, $E((\Delta y_{i,1}) v_{i,t}) = 0$, and that $\Delta y_{i,t}$ is mean stationary, $E((\Delta^2 y_{i2}) c_i) = 0$, for all $i \neq j$ and $s \neq t$. I also assume that national economic conditions x_t are strictly exogenous with respect to state-level cyberattack losses, assuming that it is unlikely that cyberattacks have driven economic conditions over this period.

Consider first the model (2) for the frequency of cyberattacks ($y_{i,t}$). I set the number of lags to $p = 2$, given that the third lag turns out not to be statistically significant (see Appendix A). I use the moment conditions

$$\begin{aligned} E(\Delta y_{i,s} \Delta v_{it}) &= 0 \quad \text{for all } i \text{ and } t-4 \leq s \leq t-5 \\ E(x_s \Delta v_{it}) &= 0 \quad \text{for all } i, s, t \\ E((\Delta^2 y_{i,t-3})(c_i + v_{it})) &= 0 \quad \text{for all } i, t \end{aligned} \tag{4}$$

Since there are more moment conditions than parameters in 17, we estimate them by minimizing their quadratic distance from zero. Estimation is done in two steps, where the variance of the moment conditions is estimated in the first step and used to weight them optimally in the second step. Furthermore, to avoid finite-sample bias in the standard errors, I apply the Windmeijer (2005) correction. This procedure produces the estimates in Table 4, with standard errors in parentheses. The diagnostic tests in the bottom rows of the table are favorable: the Hansen test of overidentifying restrictions does not reject the validity of the moment conditions in equation (17), there is the required statistically significant evidence of negative first-order serial correlation in the first-differenced residuals (e.g., standard normal test statistic of -4.3 in Column (1)), and there is no clear evidence of second-order serial correlation in the first-differenced residuals (e.g., standard normal test statistic of -1.1 in Column (1)).

The estimated coefficients on US real GDP per person and unemployment in Column (2) are similar in magnitude to (e.g., within one standard deviation of) those under the fixed effects estimator (Column (1) of Table 2), suggesting that any bias in the fixed effects estimator of coefficient β is limited, as expected. However, the coefficients on state level GSP per person and unemployment are smaller and not statistically significant using the GMM estimator. This result again emphasizes the remote nature of cyberattacks, in which national economic conditions matter more than local conditions. Columns (3) and (4) show that the lack of statistical significance of the coefficients on state level economic conditions is not driven by difficulty distinguishing them due to collinearity between real GSP per person and state level unemployment in a finite sample.

Column (5) adds national levels of digitalization, inequality, and poverty. The coefficient estimates are similar in magnitude to those of the fixed effects estimator (Column (2) of Table 2). One new feature of the GMM

Table 4: State-level frequency of cyberattacks and macroeconomic activity, estimated by GMM

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
$L(\Delta y_{i,t})$	-0.0556	-0.0538	-0.0555	-0.0549	0.109***	-0.294***	-0.359***	-0.179***
	(0.0370)	(0.0386)	(0.0368)	(0.0390)	(0.0359)	(0.0399)	(0.0392)	(0.0420)
$L^2(\Delta y_{i,t})$	-0.104***	-0.107***	-0.104***	-0.106***	-0.289***	-0.235***	-0.140***	-0.298***
	(0.0372)	(0.0387)	(0.0372)	(0.0381)	(0.0456)	(0.0400)	(0.0391)	(0.0441)
ΔUS unemp$_t$	13.18***	12.71***	13.04***	13.22***	21.77***	12.13***	11.68***	23.60***
	(0.971)	(1.099)	(1.065)	(0.983)	(1.419)	(0.791)	(0.788)	(1.235)
$\Delta \log$(US rgdppc)$_t$	5.862***	5.593***	5.874***	5.618***	9.666***	4.719***	3.300***	9.595***
	(0.772)	(1.031)	(0.790)	(1.041)	(1.084)	(0.667)	(0.584)	(0.964)
$\Delta \log$(US internet user)$_t$					1.104***			0.964***
					(0.158)			(0.133)
ΔUS inequality$_t$					0.130***			0.168***
					(0.0120)			(0.00998)
ΔUS poverty$_t$					-0.0631***			-0.0312***
					(0.00814)			(0.00882)
$\Delta \log$(CISA pp)$_t$							-0.232***	-0.242***
							(0.0233)	(0.0219)
Δstate unemp$_{i,t}$		0.604	0.179		-0.0349			-0.148
		(0.968)	(1.019)		(1.140)			(1.076)
$\Delta \log$(state rgdppc)$_{i,t}$		0.337		0.275	0.331			0.0457
		(0.432)		(0.436)	(0.475)			(0.418)
Observations	1020	1020	1020	1020	1020	867	867	867
N	51	51	51	51	51	51	51	51
AR(1)	-4.393	-4.357	-4.408	-4.347	-4.260	-4.404	-4.079	-3.921
AR(2)	-1.139	-1.011	-1.138	-1.075	1.706	0.308	-1.190	1.902
Hansen df	51	51	51	51	51	49	54	53
Hansen	50.73	50.74	50.64	50.66	50.31	50.88	50.67	49.70
p val Hansen	0.484	0.484	0.488	0.487	0.501	0.399	0.603	0.603

Standard errors in parentheses

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$

estimates is that the effect of US poverty becomes statistically significant, although it the effect is economically small—a one percentage point increase in the US poverty rate leads to a 0.06 percent reduction in the number of cyberattacks per person, when holding output, unemployment, inequality, digitalization, and cyberattack dynamics constant.

Columns (6)-(8) show that public resources devoted to cybersecurity deters malicious cyber activity. Column (6) restricts the sample from Column (1) to those years with information on the number of federal workers at CISA and NPPD, showing slight changes to the coefficient estimates. Column (7) adds the number of federal cybersecurity workers, instrumenting with the same political variables as in Section 2, and finds that a 1 percent increase in the number of workers (per person in the US) causes a 0.2 percent decrease in the number of cyberattacks per person (in both the short and long run). Column (8) shows that these relationships with national unemployment, real GDP per person, number of internet users, poverty, inequality, and cybersecurity workers hold together in one model, suggesting that no one variable is proxying for any other.

Now consider the model (3) for the severity of cyberattacks ($l_{i,t}$). I set the number of lags to $p = 3$, which helps to control the second order serial correlation of the residuals, even though the third lag ends up not being statistically significant. I use the moment conditions

$$\begin{aligned} E(\Delta l_{i,t-6}\Delta v_{it}) &= 0 \qquad \text{for all } i \\ E(x_s \Delta v_{it}) &= 0 \quad \text{for all } i, s, t \\ E((\Delta^2 l_{i,t-5})(c_i + v_{it})) &= 0 \qquad \text{for all } i, t \end{aligned} \tag{5}$$

This procedure produces the estimates in Table 5, with standard errors in parentheses. The diagnostic tests in the bottom rows of the table are acceptable: the Hansen test of overidentifying restrictions does not reject the validity of the moment conditions in equation (5), there is the required statistically significant evidence of negative first-order serial correlation in the first-differenced residuals (e.g., standard normal test statistic of -2.3 in Column (1)), and there is no clear evidence of second-order serial correlation in the first-differenced residuals (e.g., standard normal test statistic of 1.2 in Column (1)).

Column (1) finds that growth in US real GDP per person is positively associated with cyberattack severity, and is marginally statistically significant. This is consistent with an opportunity-based mechanism whereby higher levels of production, income, or digital economic activity increase the returns to cyberattacks. Column (1) finds no statistically significant relationship between changes in the US unemployment rate and the severity of cyberattacks, although the point estimate is positive.

When state-level economic conditions are added, they are not statistically significant (Column (2)). Column (4) shows that national GDP

Table 5: State-level severity of cyberattacks and macroeconomic activity, estimated by GMM

	(1)	(2)	(3)	(4)	(5)	(6)
$(\Delta l_{i,t})$	-0.103	-0.112	-0.108	-0.107	-0.247	-0.145
	(0.257)	(0.254)	(0.232)	(0.263)	(0.237)	(0.248)
$L^2(\Delta l_{i,t})$	-0.830**	-0.838**	-0.627***	-0.667***	-0.482	-0.847***
	(0.350)	(0.350)	(0.219)	(0.225)	(0.386)	(0.249)
$L^3(\Delta l_{i,t})$	-0.236	-0.244	-0.225	-0.260	-0.110	-0.303
	(0.313)	(0.309)	(0.299)	(0.325)	(0.187)	(0.300)
ΔUS unemp$_t$	5.679	3.329				
	(9.609)	(10.45)				
$\Delta \log$(US rgdppc)$_t$	13.51*	13.32	9.130***	8.401***	7.415**	12.75***
	(8.132)	(8.282)	(1.959)	(2.006)	(3.722)	(4.950)
Δstate unemp$_{i,t}$		3.198				
		(4.019)				
$\Delta \log$(state rgdppc)$_{i,t}$		0.600		0.358		
		(1.380)		(1.378)		
$\Delta \log$(US internet user)$_t$					-0.723	
					(0.653)	
ΔUS inequality$_t$					0.0608	
					(0.124)	
ΔUS poverty$_t$					0.00909	
					(0.0875)	
$\Delta y_{i,t}$						0.407
						(0.391)
$(\Delta y_{i,t})^2$						0.875
						(1.495)
Observations	459	459	459	459	459	459
N	51	51	51	51	51	51
AR(1)	-2.267	-2.262	-3.325	-3.114	-1.437	-3.005
AR(2)	1.152	1.157	1.621	1.420	0.596	1.497
Hansen df	9	9	10	11	10	8
Hansen	6.533	6.351	7.089	7.766	7.661	4.262
p val Hansen	0.686	0.704	0.717	0.734	0.662	0.833

Standard errors in parentheses

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$

is more important than state-level GSP. These results reinforce the interpretation that the severity of cyberattacks is primarily driven by national rather than local economic conditions, consistent with the highly remote nature of malicious cyber activity.

When national unemployment is removed in Column (3), the coefficient on national real GDP per person becomes more statistically significant, suggesting that the only marginal statistical significance in Column (1) could come from difficulty in distinguishing between the effects of unemployment and real GDP per person in this shorter sample (12 years of data) with notable persistence in losses over time (requiring 3 lags of the dependent variable).

Column (5) adds measures of national digitalization, poverty, and inequality to the specification from Column (3). None of these variables is statistically significantly related to cyberattack severity once aggregate economic activity and loss dynamics are controlled for. Taken together, the GMM results in Table 5 therefore suggest that the severity of cyberattacks is procyclical with respect to aggregate economic activity and is largely unrelated to national unemployment, digitalization, and local economic conditions. These findings differ from those of the fixed effects estimator, suggesting that it is important to account for dynamic panel bias in modeling the determinants of cyber losses.

Finally, Column (6) adds the frequency of cyberattacks. The coefficients on $\Delta y_{i,t}$ and $(\Delta y_{i,t})^2$ are both positive but statistically insignificant, suggesting that there is no clear evidence that the number of cyberattacks affect cyber losses. This implies that the damage function $D(O)$ is roughly linear in cyber offenses O, making marginal losses $D'(O)$ constant. In other words, the marginal value of deterrence does not change with crime volume. In this case, the number of cyberattacks that society will optimally tolerate is determined by the marginal cost curve for law enforcement.

4 Theoretical model for the frequency of cyberattacks

The empirical analyses above suggest that increases in unemployment, decreases in law enforcement, and deeper digitalization all increase the frequency of cyberattacks. This section rationalizes these findings in the simplest possible general equilibrium model of production, consumption, and cybercrime.[11] The model links the empirical findings to the literature on

[11]The model refers to 'cybercrime', but it does not distinguish between technically criminal (in which laws are broken) and other more general malicious use of computers. Not all malicious use of computers is necessarily criminalized. In the United States for example, adware, spam emails, compiling personal information on individuals, and

the economics of crime.

4.1 Firms

Firms produce a homogenous output good using labor (L), physical capital (K), and digital capital (D) under decreasing returns to scale. They face a probability γ of a cyberattack, in which case they lose fraction l of their output. Net of these losses, the representative firm produces

$$\tilde{Y} = \begin{cases} K^{\alpha_K} D^{\alpha_D} L^{\alpha_L} & \text{with probability } 1-\gamma \\ K^{\alpha_K} D^{\alpha_D} L^{\alpha_L}(1-l) & \text{with probability } \gamma \end{cases} \tag{6}$$

with $\alpha_K + \alpha_D + \alpha_L < 1$ and its expected production (net of losses to criminals) is

$$Y = K^{\alpha_K} D^{\alpha_D} L^{\alpha_L}(1-\gamma l). \tag{7}$$

Firms are risk-neutral and therefore maximize expected net profit

$$PY - wL - r(K+D) \tag{8}$$

where P is the output price, w is the wage, and r is the required return on (physical or digital) capital, which is supplied to firms perfectly elastically. Firms are atomistic and therefore take the probability of cyberattacks, γ, as given.

Firms' first-order conditions give the following relative demand functions

$$\begin{array}{rcl} K & = & \frac{\alpha_k}{\alpha_D} D, \\ D & = & \frac{\alpha_D}{\alpha_L} \frac{w}{r} L, \end{array} \tag{9}$$

and labor demand is

$$L = \alpha_K^{\frac{\alpha_K}{\alpha_0}} \alpha_D^{\frac{\alpha_D}{\alpha_0}} \alpha_L^{\frac{1-\alpha_D-\alpha_K}{\alpha_0}} w^{\frac{\alpha_D+\alpha_K-1}{\alpha_0}} P^{\frac{1}{\alpha_0}} r^{\frac{-\alpha_D-\alpha_K}{\alpha_0}} (1-\gamma \mathrm{l})^{\frac{1}{\alpha_0}}, \tag{10}$$

where $\alpha_0 = 1 - \alpha_K - \alpha_D - \alpha_L$.

4.2 Individuals

There is a unit mass of risk-neutral individuals who choose between participating in the labor market and engaging in cybercrime, as in Furlong (1987) and Sah (1991). Denote the share of individuals that choose to engage in cybercrime, called the *cybercrime rate*, by q. If an individual chooses to participate in the labor market, they face a probability u of

creating fake news are not criminalized. This general treatment is consistent with the literature on the economics of crime.

being unemployed. Labor supply is the fraction of individuals that are not engaged in cybercrime or unemployed:

$$L = (1 - q). \tag{11}$$

If an individual is employed, they supply a unit of labor at wage w, which can be used to purchase w/P units of output for consumption. Therefore, the expected utility from participating in the labor market is

$$\frac{w}{P}(1 - u). \tag{12}$$

If an individual engages in cybercrime, they earn the average expected output per criminal that is stolen. The expected loss from getting caught is f, which is the product of the probability of getting caught and the associated penalty (e.g., fine or imprisonment), expressed as a fraction of the amount stolen. Then the expected utility from cybercrime is

$$\frac{\gamma}{q} l K^{\alpha_K} D^{\alpha_D} L^{\alpha_L} (1 - f). \tag{13}$$

Suppose that the probability of a successful cyberattack is

$$\gamma = q^{\sigma_q} \left(\frac{D}{1 + D} \right)^{\sigma_D} \tag{14}$$

with $0 < \sigma_q, \sigma_D < 1$. This specification implies that the risk to the firm of a cyberattack (γ) increases with the level of digitalization of the firm (D) and the cybercrime rate q.

An important feature of (14) is that γ increases slower than q, so that γ/q falls as q rises. This ensures that there will always be some crime in equilibrium (i.e., $q > 0$), because the expected earnings for the average cybercriminal would be arbitrarily high at sufficiently low crime rates. At low levels of cybercrime therefore (i.e., when q is small), the marginal returns to engaging in cybercrime will be larger than the real wage, which will encourage more individuals to choose cybercrime over work. The cybercrime rate would therefore increase. Equation (14) also ensures that not everyone will become criminals in equilibrium (i.e., $q < 1$), because the expected earnings for the average cybercriminal (which are proportional to γ/q) would become diluted as more individuals become criminals, with earnings becoming arbitrarily low at sufficiently high crime rates. At high crime rates therefore, the real wage would be more attractive to the individual than the return from cybercrime, and more individuals would choose work over cybercrime, thus reducing the cybercrime rate. In equilibrium, cybercrime co-exists with work, with individuals being indifferent at the

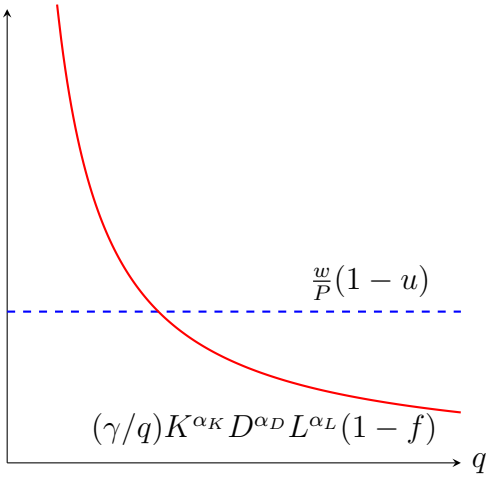


Figure 3: The equilibrium cybercrime rate will equate the expected utility from work (dashed blue line) and cybercrime (solid red line), so that individuals are indifferent between the two at the margin.

margin between participating in the labor market and engaging in cybercrime. The fraction of individuals that engage in cybercrime, q, therefore adjusts to equate (12) with (13), as shown in Figure 3. This gives

$$q = \left(\frac{\left(\frac{D}{1+D}\right)^{\sigma_D} l K^{\alpha_K} D^{\alpha_D} L^{\alpha_L} (1-f)}{\frac{w}{P}(1-u)} \right)^{\frac{1}{1-\sigma_q}} \tag{15}$$

4.3 Equilibrium in the short run

The labor market clears when the wage rate w equates the labor demanded by firms (10) to the labor supplied by individuals (11). This wage rate satisfies

$$\begin{aligned} w^{1-\alpha_D-\alpha_K} = {} & \alpha_K^{\alpha_K}\, \alpha_D^{\alpha_D}\, \alpha_L^{1-\alpha_D-\alpha_K}\, P\, r^{-\alpha_D-\alpha_K}\, (1-q)^{-\alpha_0} \\ & \times \left(1 - q^{\sigma_q} \left(\frac{D}{1+D}\right)^{\sigma_D} l\right). \end{aligned} \tag{16}$$

In the short run, which is relevant to compare with data based on year-to-year fluctuations, output prices are likely to be sticky. I therefore analyze the case of fixed prices, $P = 1$. In this case, the goods market need not clear, and resources could be temporarily under- or over-utilized.

Equilibrium in this economy is a set $\{K, D, L, w, q, \gamma\}$ that satisfies the labor market clearing condition (16), the indifference criterion between

work and cybercrime (15), and the demands for physical and digital capital (9) for a given set of parameter values $\{\alpha_K, \alpha_D, \alpha_L, r, l, \delta, u, \sigma_q, \sigma_D, f, P\}$.

4.4 Calibration and comparative statics

To examine how unemployment, law enforcement, and digitalization affect cyber risk in this model, I calibrate a baseline version of the model to match conditions in the US (Table 6). In this calibration, the model is able to reproduce a high rate of cyberattacks, $\gamma = 0.4$, and a low rate of cybercrime, $q = 0.0066$.

4.4.1 The effect of unemployment on cybercrime

By reducing the return to work, a higher unemployment rate encourages more people to choose cybercrime over work, thus restricting labor supply (Figure 4a) and increasing the cybercrime rate (Figure 4c). The higher cybercrime rate in turn increases the probability of firms facing cyberattacks (Figure 4d), which increases losses for firms. These increased losses reduce the marginal product of labor and the wage rate, outweighing the reduction in labor supply (Figure 4b). The reduced wage rate further reduces the return to work, leading even more people to choose cybercrime over work and amplifying the above mechanism.

4.4.2 The effect of law enforcement on cybercrime

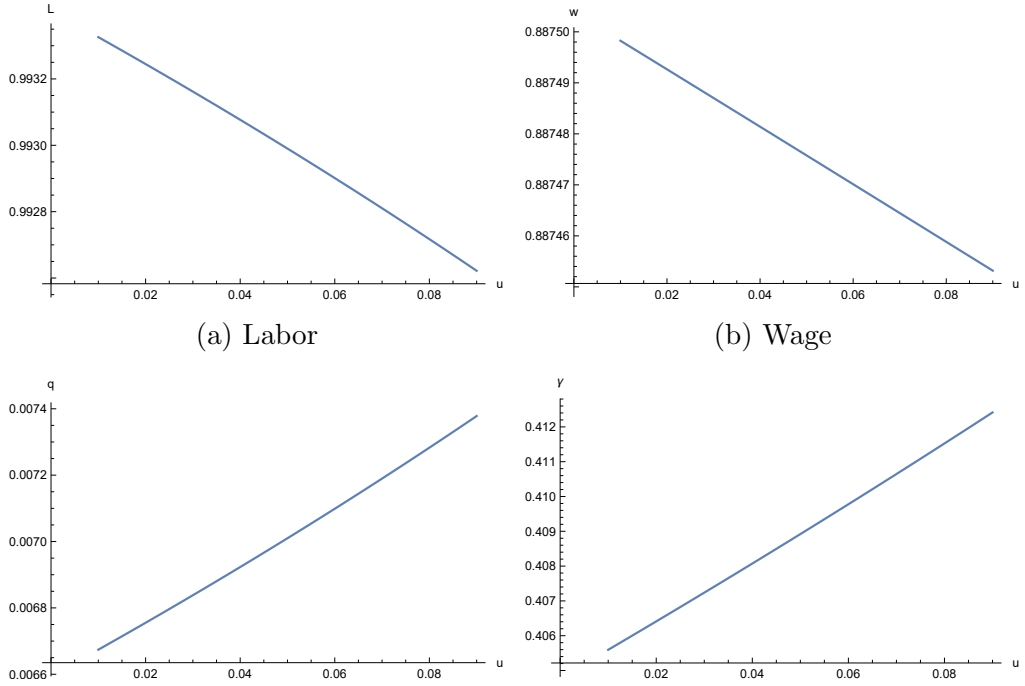
Tougher law enforcement, which summarizes both the probability of catching cybercriminals and the penalties imposed on those caught, reduces the returns to engaging in cybercrime, leading to lower cybercrime rates and lower probabilities of firms facing cyberattacks (Figure 5c and 5d). The lower returns to cybercrime encourage more individuals to choose work instead, which increases labor supply (Figure 5a). The increase in labor supply raises economic output, which leads firms to increase their demand for all factors of production, including workers. These labor demand effects outweigh the labor supply effects, so the wage rate increases (Figure 5b).

4.4.3 The effect of digitalization on cybercrime

To simulate increases in digitalization without changing the overall degree of returns to scale of the economy, we increase α_D while keeping $\alpha_K + \alpha_D$ constant. The increase in α_D leads firms to increase their demand for digital capital D, substituting digital capital for physical capital and, initially, labor (Figure 6a). This reduced demand for labor pushes more people into cybercrime (Figure 6c) and increases the probability of a cyberattack (Figure 6d).

Table 6: Calibrated parameter values for the analysis of comparative statics.

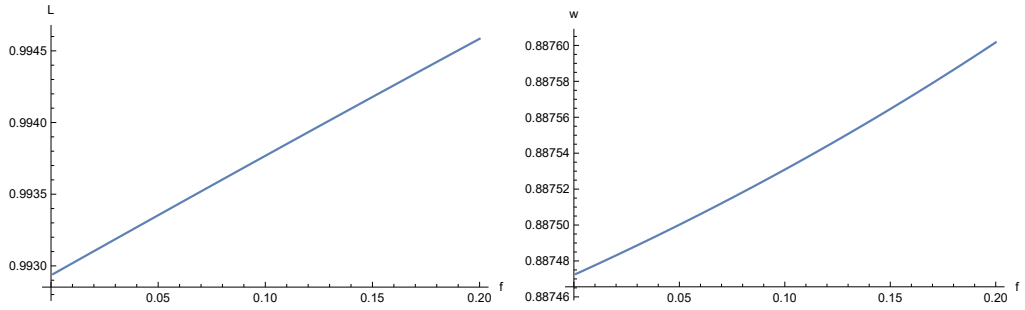
Parameter	Calibration	Explanation
α_L	0.6	Labor share of value added for the US from the Penn World Tables 10.01.
α_D	0.12	Digital economy share of value added, from the US Bureau of Economic Analysis.
α_K	0.23	$0.23 = 0.95 - 0.6 - 0.12$
r	0.088	Average weighted cost of capital at end-2022 from Mauboussin and Callahan (2023).
u	0.037	Average US unemployment rate in 2019 from the US Bureau of Labor Statistics.
l	0.01	This is the ratio of the cost of malicious cyber activity of 0.4 percent of GDP, which is the middle of the range of estimates provided by the Council of Economic Advisers (2018), and the 43 percent of firms suffering a cyberattack in a year (due to Hiscox (2021)).
f	0.02	This is the product of the probability of being caught and the penalty if caught. The probability of being caught is set to be the conviction rate of around 0.1 percent per year, based on the ratio of 1177 convictions for cybercrimes between 2006 and 2010 (Marcum, Higgins, and Tewksbury 2011) to the total number of complaints to the FBI's Internet Crime Complaints Center over the same period. The penalty if caught is set to be an average of 20 years' wages, given statutory sentences in the US of up to 40 years for cybercrime. One year's wage is close to $w = 1$ in the model.
σ_q, σ_D	1/6	Chosen to achieve $\gamma = .40 \approx 0.43$, which is the proportion of firms suffering a cyberattack in a year (due to Hiscox (2021)).



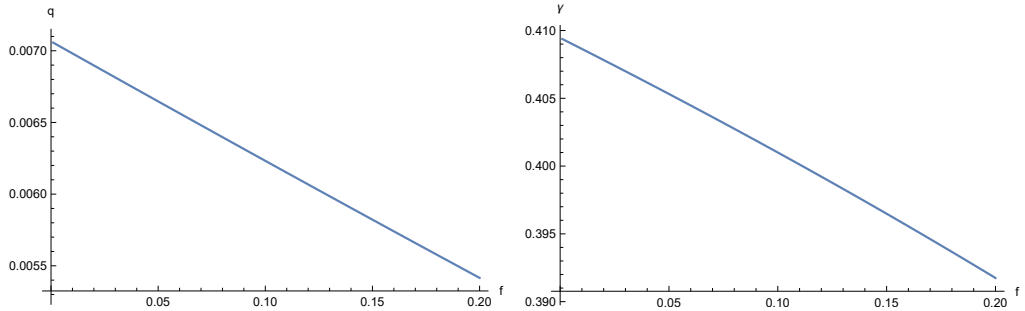
(a) Labor (b) Wage

(c) Cybercrime rate (d) Probability of cyberattack

Figure 4: Comparative statics: The effect of the unemployment rate (u) on the equilibrium quantity of labor (L), wage (w), cybercrime rate (q), and probability of cyberattack (γ).

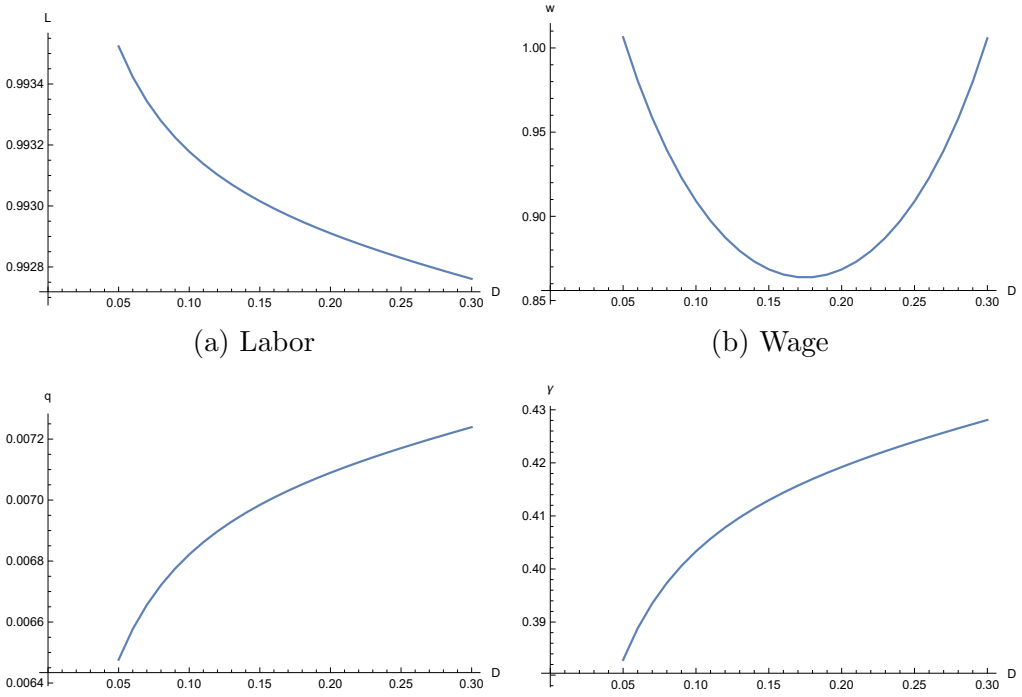


(a) Labor (b) Wage



(c) Cybercrime rate (d) Probability of cyberattack

Figure 5: Comparative statics: The effect of law enforcement (f) on the equilibrium quantity of labor (L), wage (w), cybercrime rate (q), and probability of cyberattack (γ). The law enforcement parameter captures both the probability of catching cybercriminals and the penalties imposed on those caught.



(a) Labor (b) Wage

(c) Cybercrime rate (d) Probability of cyberattack

Figure 6: Comparative statics: The effect of digitalization (α_D) on the equilibrium quantity of labor (L), wage (w), cybercrime rate (q), and probability of cyberattack (γ).

As α_D increases however, and firms substitute more digital capital for physical capital and labor, this substitution gets more difficult, due to the shape of the Cobb-Douglas production function. The marginal productivity of labor decreases at a slower rate and eventually stabilizes. After this point, further increases in α_D cause the marginal productivity of labor to increase, because digital capital D increases by a large amount compared to the decrease in physical capital K, and labor L is at a low level. Despite the higher marginal productivity of labor, firms continue to substitute digital capital for labor. This substitution, together with the higher rate of digitalization in the economy, continues to drive more people into cybercrime (Figure 6c) and increase the probability of a cyberattack (Figure 6d).

5 Conclusion

I compile new data on the frequency and severity of cyberattacks across US states and time. Using a range of econometric estimators, I find that higher unemployment, greater aggregate output, increased digitalization, and wider income inequality are each associated with more frequent cyber-

attacks, whereas stronger law enforcement capacity in cybersecurity leads to fewer cyberattacks.

These patterns align closely with the economic theory of crime (Becker 1968; Ehrlich 1973) as applied to the cyber domain. Higher unemployment motivates more individuals to engage in cybercrime and higher output provides more opportunity for theft, damage, and disruption. At the same time, stronger law enforcement reduces the expected return from engaging in cybercrime.

Cyberattacks have two unique features that distinguish them from other types of crime. I find evidence, first, that they increase following higher digitalization. Second, I find that they are driven more by national than local economic conditions, which is consistent with the fact that they happen remotely and across state lines.

Notably, I also document that the average loss per cyberattack increases with overall economic output, indicating that higher output not only attracts more attacks but also raises the stakes of each incident. At the same time, the evidence suggests that average losses do not systematically increase with the volume of cyberattacks, implying that marginal social damage is approximately constant as attack volumes rise. Together, these findings extend standard crime theory by showing that, while the severity of harm can endogenously scale with aggregate income, the marginal value of deterrence need not increase with the frequency of attacks.

I rationalize the drivers of cyberattacks in a simple general equilibrium model. In equilibrium, individuals allocate effort between lawful work and cybercrime, and firms invest in both physical and digital capital while facing a risk of attack. Comparative statics reveal that a higher unemployment rate induces more people to opt for cybercrime over formal work, stronger punishment or higher probability of capture deters cyber offenses, and greater digitalization increases the economy's exposure to cyberattacks.

These findings carry several implications for economic theory and policy. First, the fact that macroeconomic fluctuations influence cyberattack frequency implies that cyber risk should be viewed as partly systemic and non-diversifiable within a single country. Insuring cyber risk may therefore call for cross-border financial arrangements, analogous to natural disasters or economic crises.

Second, public cybersecurity employment curbs cybercrime and may be below socially optimal levels. A back-of-the-envelope calculation suggests that a 1 percent increase in such employment avoids economic losses from cyberattacks of at least US$ 100 million in 2023 dollars, which equals the lower bound of annual costs of cyberattacks of 0.3 percent of GDP from Council of Economic Advisers (2018) multiplied by my estimated coefficient of 0.2 from Table 4. By contrast, a 1 percent increase in cybersecurity employment would cost at most US$ 25 million, assuming conservatively

that the entire 2023 CISA budget went to staffing.

Third, the results provide further reason to support stabilization and redistribution policies. By dampening severe recessions and preventing large spikes in unemployment, policymakers may mitigate accompanying surges in cybercrime. Income redistribution that successfully reduces inequality could also deter cybercrime.

Future research could consider potential feedback loops between cyberattacks and economic activity, which is likely to become more relevant as the economy becomes ever more digital, with the rise of artificial intelligence and the proliferation of the Internet of Things. If economic downturns motivate even more people to turn to cybercrime in future, this could amplify downturns.

References

Abdymomunov, Azamat, Filippo Curti, and Atanas Mihov (2020). "US banking sector operational losses and the macroeconomic environment". In: *Journal of Money, Credit and Banking* 52.1, pp. 115–144.

Aldasoro, Iñaki et al. (2020). "Operational and cyber risks in the financial sector". In.

— (2022). "The drivers of cyber risk". In: *Journal of Financial Stability* 60, p. 100989.

Anderson, Ross and Tyler Moore (2006). "The economics of information security". In: *Science* 314.5799, pp. 610–613.

Arellano, Manuel and Stephen Bond (1991). "Some tests of specification for panel data: Monte Carlo evidence and an application to employment equations". In: *The Review of Economic Studies* 58.2, pp. 277–297.

Arellano, Manuel and Olympia Bover (1995). "Another look at the instrumental variable estimation of error-components models". In: *Journal of Econometrics* 68.1, pp. 29–51.

Becker, Gary S (1968). "Crime and punishment: An economic approach". In: *Journal of Political Economy* 76.2, pp. 169–217.

Blundell, Richard and Stephen Bond (1998). "Initial conditions and moment restrictions in dynamic panel data models". In: *Journal of Econometrics* 87.1, pp. 115–143.

Cobos, Estefania Vergara et al. (2024). "A review of the economic costs of cyber incidents". In: *World Bank, Washington, DC, USA, Rep* 193919.

Council of Economic Advisers (2018). *The cost of malicious cyber activity to the U.S. economy*. Tech. rep. White House.

Crosignani, Matteo, Marco Macchiavelli, and André F Silva (2023). "Pirates without borders: The propagation of cyberattacks through firms' supply chains". In: *Journal of Financial Economics* 147.2, pp. 432–448.

Driscoll, John C and Aart C Kraay (1998). "Consistent covariance matrix estimation with spatially dependent panel data". In: *Review of Economics and Statistics* 80.4, pp. 549–560.

Ehrlich, Isaac (1973). "Participation in illegitimate activities: A theoretical and empirical investigation". In: *Journal of Political Economy* 81.3, pp. 521–565.

Eling, Martin and Kwangmin Jung (2022). "Heterogeneity in cyber loss severity and its impact on cyber risk measurement". In: *Risk Management* 24.4, p. 273.

Furlong, William J (1987). "A general equilibrium model of crime commission and prevention". In: *Journal of Public Economics* 34.1, pp. 87–103.

Hiscox (2021). *Cyber Readiness Report*. Hiscox.

Holtz-Eakin, Douglas, Whitney Newey, and Harvey S Rosen (1988). "Estimating vector autoregressions with panel data". In: *Econometrica*, pp. 1371–1395.

International Monetary Fund (2024). *Global Financial Stability Report, April 2024: Cyber Risk–A Growing Concern for Macrofinancial Stability*. Tech. rep. International Monetary Fund.

Internet Crime Complaint Center (2010). *2010 Internet Crime Report*. Tech. rep. Federal Bureau of Investigation.

Jamilov, Rustam, Hélène Rey, and Ahmed Tahoun (2021). *The anatomy of cyber risk*. Tech. rep. National Bureau of Economic Research.

Judson, Ruth A and Ann L Owen (1999). "Estimating dynamic panel data models: a guide for macroeconomists". In: *Economics Letters* 65.1, pp. 9–15.

Kamiya, Shinichi et al. (2021). "Risk management, firm reputation, and the impact of successful cyberattacks on target firms". In: *Journal of Financial Economics* 139.3, pp. 719–749.

Kelly, Morgan (2000). "Inequality and crime". In: *Review of Economics and Statistics* 82.4, pp. 530–539.

Marcum, Catherine D, George E Higgins, and Richard Tewksbury (2011). "Doing time for cyber crime: An examination of the correlates of sentence length in the United States". In: *International Journal of Cyber Criminology* 5.2.

Mauboussin, Michael and Dan Callahan (Feb. 2023). *Cost of capital—A practical guide to measuring opportunity cost*. Tech. rep. Morgan Stanley Investment Management.

Moore, Tyler, Richard Clayton, and Ross Anderson (2009). "The economics of online crime". In: *Journal of Economic Perspectives* 23.3, pp. 3–20.

Nickell, Stephen (1981). "Biases in dynamic models with fixed effects". In: *Econometrica: Journal of the Econometric Society*, pp. 1417–1426.

Office of Financial Research (2017). "Cybersecurity and Financial Stability: Risks and Resilience". In: *OFR Viewpoint* 17-01.

Olea, José Luis Montiel and Carolin Pflueger (2013). "A robust test for weak instruments". In: *Journal of Business & Economic Statistics* 31.3, pp. 358–369.

Sah, Raaj K (1991). "Social osmosis and patterns of crime". In: *Journal of Political Economy* 99.6, pp. 1272–1295.

Windmeijer, Frank (2005). "A finite sample correction for the variance of linear efficient two-step GMM estimators". In: *Journal of Econometrics* 126.1, pp. 25–51.

A Robustness checks

This appendix documents a set of robustness checks designed to assess the sensitivity of the main empirical results to alternative specifications, lag structures, and estimators. The robustness exercises confirm the qualitative conclusions of the paper.

A.1 Alternative lag lengths in fixed effects models

Table 7 reports robustness checks for the fixed effects estimates of state-level cyberattack frequency. Column (1) of Table 7 reproduces the baseline specification from Column (1) of Table 2 in the main text, with two lags of the dependent variable. The estimated coefficients on national unemployment and national real GDP per person are positive and statistically significant, while the coefficients on state-level unemployment and state-level real GSP per person are smaller in magnitude. Column (2) of Table 7 adds a third lag of the dependent variable. The coefficient on the third lag is not statistically significant, and the estimated coefficients on national unemployment and national real GDP per person remain positive and statistically significant, within one standard deviation of their values in Column (1). By contrast, the coefficients on state-level unemployment and state-level real GSP per person decline in magnitude and lose statistical significance. This pattern suggests that the effects of national economic conditions are stable, whereas the effects of local economic conditions are more sensitive to dynamic specification.

Columns (3) and (4) repeat this exercise for the specification that additionally includes measures of national digitalization, inequality, and poverty (corresponding to Column (2) of Table 2 in the main text). Again, adding a third lag of the dependent variable does not materially affect the estimated coefficients on national unemployment, national real GDP per person, digitalization, or inequality. These coefficients remain positive and statistically

Table 7: Robustness checks for state-level frequency of cyberattacks and macroeconomic activity, estimated by fixed effects, with different lag lengths

	(1)	(2)	(3)	(4)	(5)	(6)
$L(\Delta y_{i,t})$	−0.024	−0.163*	0.018	−0.174***	−0.272***	−0.264***
	(0.122)	(0.085)	(0.118)	(0.048)	(0.055)	(0.056)
$L^2(\Delta y_{i,t})$	−0.024	−0.123	−0.117	−0.264***	−0.240***	−0.241***
	(0.106)	(0.077)	(0.125)	(0.064)	(0.059)	(0.070)
$L^3(\Delta y_{i,t})$		−0.011		−0.074	−0.143**	−0.156**
		(0.081)		(0.061)	(0.058)	(0.074)
$L^4(\Delta y_{i,t})$						−0.044
						(0.067)
ΔUS unemp$_t$	12.761***	12.149***	21.841***	25.988***		
	(2.752)	(2.722)	(3.422)	(3.349)		
$\Delta \log$(US rgdppc)$_t$	6.171**	5.075**	10.584***	12.733***		
	(2.569)	(2.129)	(2.018)	(2.275)		
Δstate unemp$_{i,t}$	1.342**	0.725	0.915	0.141	0.718*	0.812**
	(0.604)	(0.472)	(0.723)	(0.362)	(0.424)	(0.367)
$\Delta \log$(state rgdppc)$_{i,t}$	0.788**	0.508	0.733*	0.389	0.483**	0.494**
	(0.380)	(0.340)	(0.429)	(0.277)	(0.211)	(0.227)
$\Delta \log$(US internet user)$_t$			1.181***	1.144***		
			(0.413)	(0.335)		
ΔUS inequality$_t$			0.116**	0.167***		
			(0.046)	(0.034)		
ΔUS poverty$_t$			−0.047	−0.021		
			(0.036)	(0.031)		
state FE:	yes	yes	yes	yes	yes	yes
time FE:	no	no	no	no	yes	yes
partial R-squared:	0.255	0.339	0.34	0.467	0.035	0.094
N	51	51	51	51	51	51
T	20	19	20	19	19	18
Observations	1,020	969	1,020	969	969	918
R^2	0.260	0.347	0.345	0.476	0.577	0.587

Note: *p<0.1; **p<0.05; ***p<0.01
Driscoll and Kraay (1998) standard errors shown in parentheses.

significant, while the coefficients on state-level variables become smaller and less precisely estimated.

Columns (5) and (6) introduce time fixed effects and drop national macroeconomic variables, corresponding to Column (3) of Table 2 in the main text. Column (5) includes three lags of the dependent variable, while Column (6) adds a fourth lag, which is not statistically significant. Comparing Columns (5) and (6), the coefficients on state-level unemployment and state-level real GSP per person remain positive and statistically significant in both specifications, with similar magnitudes—within one standard deviation. This indicates that the estimated effects of state-level economic conditions in the specification with time fixed effects are robust to allowing for additional dynamics.

A.2 Robustness of system GMM estimates for cyberattack frequency

Table 8 reports robustness checks for the system GMM estimates of cyberattack frequency. Column (1) reproduces the baseline GMM specification from Column (1) of Table 4 in the main text. Column (2) adds a third lag of the dependent variable to the specification. The third lag is not statistically significant. The coefficients on national unemployment and national real GDP per person are robust in that they remain positive and statistically significant, although their point estimates reduce somewhat.

Column (3) re-estimates the baseline specification using a one-step GMM estimator instead of the two-step estimator. The estimated coefficients on national unemployment and national real GDP per person remain positive, statistically significant, and close in magnitude to those in Column (1), which suggests that the baseline results are not sensitive to the choice of GMM weighting matrix or to finite-sample corrections in the two-step procedure.

Column (4) checks the robustness of the estimation in Column (2) of Table 4 to using the following alternative set of moment conditions

$$\begin{aligned} E(\Delta y_{i,s}\Delta v_{it}) &= 0 \quad \text{for all } i \text{ and } t-3 \leq s \leq t-4 \\ E(x_s \Delta v_{it}) &= 0 \quad \text{for all } i, s, t \\ E((\Delta^2 y_{i,t-2})(c_i + v_{it})) &= 0 \quad \text{for all } i, t \end{aligned} \tag{17}$$

Column (4) shows that the coefficients on national unemployment and national real GDP per person remain positive and statistically significant, although their point estimates reduce. The coefficients on state-level unemployment and state-level real GSP per person remain small and statistically insignificant. This reinforces the conclusion that cyberattack frequency responds primarily to national rather than local economic conditions.

A.3 Robustness to an alternative measure of cyberattacks: data breaches

As a robustness check, we re-estimate the aggregate US regressions using data breaches from the Identity Theft Resource Center (ITRC), which capture successful, reportable compromises of organizations rather than attempted or reported cyber incidents. Table 9 shows the results, again using finite sample inference—the tests do not reject homoskedasticity and normality of the residuals.[12]

[12]No lags of the dependent variable are needed to address heteroskedasticity. When included, they are not statistically significant.

Table 8: Robustness checks for state-level frequency of cyberattacks and macroeconomic activity, estimated by GMM

	(1)	(2)	(3)	(4)
$L(\Delta y_{i,t})$	-0.0556	-0.0857*	-0.0563	0.214***
	(0.0370)	(0.0492)	(0.0356)	(0.0298)
$L^2(\Delta y_{i,t})$	-0.104***	-0.146***	-0.103***	-0.0527
	(0.0372)	(0.0432)	(0.0372)	(0.0361)
$L^3(\Delta y_{i,t})$		0.0376		
		(0.0289)		
ΔUS unemp$_t$	13.18***	10.98***	13.21***	8.212***
	(0.971)	(1.103)	(0.893)	(1.080)
$\Delta \log$(US rgdppc)$_t$	5.862***	3.757***	5.863***	1.840**
	(0.772)	(0.950)	(0.737)	(0.920)
Δstate unemp$_{i,t}$				0.903
				(1.120)
$\Delta \log$(state rgdppc)$_{i,t}$				0.513
				(0.473)
Observations	1020	969	1020	1020
N	51	51	51	51
AR(1)	-4.393	-4.437	-4.742	-4.777
AR(2)	-1.139	0.0343	-1.735	-0.341
Hansen df	51	50	51	54
Hansen	50.73	50.83	50.73	50.78
p val Hansen	0.484	0.441	0.484	0.599

Standard errors in parentheses

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$

The results in Table 9 confirm the importance of national economic conditions in driving data breaches. However, there are two differences. First, it takes two years for unemployment and real GDP per person to affect data breaches, whereas they have an immediate effect on FBI cyberattacks. Second, when the variables enter the specification individually, the coefficient on unemployment is negative and the coefficient on real GDP per person is positive. The signs of these two coefficients are opposite of those in Table 1 Columns (1) and (2), suggesting that data breaches respond differently to macroeconomic conditions than the broad FBI measure of cyberattack activity. Breaches reflect the realization of high-value attacks rather than marginal participation in cybercrime.

When unemployment and real GDP per person are included jointly in the same regression (Column (3)), both coefficients become positive, but only real GDP per person remains statistically significant. This result indicates that the negative coefficient on unemployment in the single-variable specification reflects omitted-variable bias: unemployment is negatively correlated with aggregate income, which is the primary driver of data breaches. Once real GDP per person is controlled for, unemployment no longer has independent explanatory power. The positive and statistically significant coefficient on real GDP per person in the joint regression (Column (3)) agrees with the state-level evidence based on fixed-effects and GMM estimators (Tables 2 and 4). Intuitively, data breaches depend primarily on the value of targets, which is more tightly linked to aggregate income than to labor market slack. By contrast, unemployment mainly affects the extensive margin of low-threshold cyber activity, such as attempted attacks, rather than the realization of large, reportable breaches.

A.4 Robustness to asymptotic standard errors

Table 10 shows a version of Columns (1)-(3) of Table 1 using asymptotic, Newey–West standard errors. The coefficients and their statistical significance agrees with those in Tbale 1.

B Data sources and construction

Table 11 summarizes variable definitions and sources. Cyberattack data are from annual Internet Crime Reports published by the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) between 2001 and 2024. IC3 reports the number of complaints and total reported monetary losses in each state and year. Complaints are used as a proxy for cyberattack frequency. Population data are from the Bureau of Economic Analysis (BEA) via Federal Reserve Economic Data (FRED). The cyberattack rate $y_{i,t}$ is defined as the log of complaints per 100,000 people.

Table 9: Robustness check: Replacing FBI cyberattacks with data breaches

	(1)	(2)	(3)
$L^2(\Delta \text{US unemp}_t)$	-8.855^{**}		6.790
	(4.040)		(8.427)
$L^2(\Delta \log(\text{US rgdppc})_t)$		9.437^{***}	14.527^{*}
		(3.055)	(7.030)
Constant	0.147^{**}	0.032	-0.028
	(0.065)	(0.071)	(0.103)
Method:	OLS	OLS	OLS
Breusch-Pagan p-value:	0.8823	0.9366	0.979
Shapiro-Wilk p-value:	0.44	0.4899	0.4926
Observations	19	19	19
R^2	0.220	0.360	0.385
Note:		*p<0.1; **p<0.05; ***p<0.01	

Cyberattack severity is measured as average losses per complaint. Nominal losses are deflated using the US consumer price index (CPIAUCSL, FRED) and expressed in constant 2015 dollars. The severity $l_{i,t}$ is the log of real average losses per cyberattack.

National macroeconomic variables are from FRED. The US unemployment rate is UNRATE. Real GDP per person is constructed from real GDP (GDPCA) divided by population (B230RC0A052NBEA). State unemployment rates and real gross state product (RGSP) are both from FRED. State real GDP per capita is RGSP divided by state population.

Digitalization is proxied by the number of internet users in the United States (ITNETUSERP2USA, World Bank via FRED). Income inequality is measured by the US Gini coefficient (SIPOVGINIUSA), and poverty by the national poverty rate (PPAAUS00000A156NCEN), both from the US Census Bureau via FRED.

Public cybersecurity resources are measured using staffing data for the Cybersecurity and Infrastructure Security Agency (CISA) and its predecessor, the National Protection and Programs Directorate (NPPD), from annual Budget in Brief reports of the US Department of Homeland Security. Staffing levels are divided by national population.

Summary statistics are reported in Table 12. All variables are annual.

Table 10: Robustness check: Replacing finite sample inference with asymptotic, Newey–West standard errors

	(1)	(2)	(3)
$L(\Delta y_{i,t})$	0.340^{**}	0.559^{**}	0.305^{*}
	(0.141)	(0.207)	(0.159)
$L^2(\Delta y_{i,t})$	-0.352^{*}	-0.444^{**}	-0.337
	(0.187)	(0.159)	(0.199)
$L^3(\Delta y_{i,t})$	0.265^{**}	0.328^{**}	0.249^{*}
	(0.108)	(0.114)	(0.122)
$L^4(\Delta y_{i,t})$	-0.219	-0.210	-0.216
	(0.159)	(0.145)	(0.168)
ΔUS unemp$_t$	6.273^{***}		7.245
	(1.832)		(5.635)
$\Delta \log$(US rgdppc)$_t$		-4.750^{**}	0.876
		(2.033)	(4.161)
Constant	0.072^{*}	0.113^{*}	0.064
	(0.034)	(0.054)	(0.037)
Method:	OLS	OLS	OLS
Observations	19	19	19
R^2	0.582	0.524	0.583
Note:		*p<0.1; **p<0.05; ***p<0.01	

Table 11: Variable definitions and sources

Variable	Data source	Description
$\Delta y_{i,t}$	FBI IC3; FRED population	Year-to-year change in log cyberattack rate per 100,000 people in state i
$\Delta \ell_{i,t}$	FBI IC3; CPI (FRED)	Year-to-year change in log real average loss per cyberattack in state i (2015 USD)
Δ US unemp$_t$	FRED (UNRATE)	Year-to-year change in U.S. unemployment rate (percentage points)
$\Delta \log$(US rgdppc)$_t$	FRED (GDPCA, population)	Growth rate of U.S. real GDP per capita
Δ state unemp$_{i,t}$	FRED (state UR)	Year-to-year change in state unemployment rate (percentage points)
$\Delta \log$(state rgdppc)$_{i,t}$	FRED (RGSP, POP)	Growth rate of real gross state product per capita
$\Delta \log$(US internet users)$_t$	World Bank / FRED	Growth rate of number of internet users in the United States
Δ US poverty$_t$	U.S. Census / FRED	Year-to-year change in U.S. poverty rate (percentage points)
Δ US inequality$_t$	U.S. Census / FRED	Year-to-year change in U.S. income Gini coefficient
$\Delta \log$(CISA pp)$_t$	DHS budget data	Growth rate of federal cybersecurity staff per capita (CISA/NPPD)

Table 12: Summary statistics for state-level data

variable	mean	stdev	min	max	N	range
$\Delta y_{i,t}$	0.1	0.3	-1.2	1.2	51	2002-2024
$\Delta l_{i,t}$	0.2	0.5	-2.3	2.3	52	2012-2024
ΔUS unemp$_t$	0	0	0	0	52	2001-2024
$\Delta \log$(US rgdppc)$_t$	0	0	0	0.1	52	2001-2024
Δstate unemp$_{i,t}$	0	0	-0.1	0.1	52	1996-2024
$\Delta \log$(state rgdppc)$_{i,t}$	0	0	-0.1	0.2	51	1998-2024
$\Delta \log$(US internet user)$_t$	0	0.1	0	0.2	52	2001-2023
ΔUS poverty$_t$	0.1	0.5	-0.8	1.1	52	2001-2023
ΔUS inequality$_t$	0.1	0.7	-1.9	2	52	2001-2023
$\Delta \log$(CISA pp)$_t$	0.1	0.2	-0.7	0.5	52	2007-2024