Introducing the IT Economics Department

Nir Kshetri
University of North Carolina at Greensboro

Editor:
Nir Kshetri, University of North Carolina at Greensboro; nbkshetr@uncg.edu

Welcome to the new IT Economics department, which seeks to advance the understanding of various microeconomic and macroeconomic issues that IT managers need to examine in their decisions to adopt and implement information and communications technology (ICT)-related systems, services, processes, and practices.

Microeconomic forces operate at the level of an adopting unit or organization. These forces influence how likely or unlikely organizations are to adopt a particular system, service, process, or practice. Put differently, they affect how organizations evaluate the costs and benefits of ICT-related systems, services, processes, and practices. For instance, when making a decision to implement an ICT system, IT managers need to take into account costs and benefits associated with ownership of the system, making effective use of the system, learning and switching to the system, and the system's compatibility with existing systems. Of course, the costs and benefits of implementing an ICT solution will vary across organizations of different sizes and in different industries.

Macro-level forces also influence the adoption of ICT-related systems, services, processes, and practices.[1] These are external forces such as the regulations, rules, and policies enacted by national, regional, and local governments.[2] Thus, the political economy of development and use of ICT-related systems, services, processes, and practices will be one of the key focus areas of this department. Other major macro-level forces include the availability of ICT infrastructures and skills, consumer preferences, and external threats (for example, from malware and cybercriminals). This department will also consider intermediate-level forces such as those related to actions of competitors and pressure from trade association and industry groups as well as from value-delivery networks (for example, supply-chain partners).[3]

A related focus of this department concerns increasing returns and externalities. W.B. Arthur noted that "increasing returns are … mechanisms of positive feedback that operate—within markets, businesses, and industries—to reinforce that which gains success or aggravate that which suffers loss."[4] This approach would help explain how firms, innovations, industries, and the environment influence one another.[5] The law of increasing returns argues that economies of scale, decreasing costs, and feedback mechanisms lead to further success for already successful entities. Articles published in this department, for instance, can explore the effects of increasing returns in an ICT industry and analyze whether self-reinforcing feedback provided by institutions, industry, and the market might allow an IT system to gain an edge over competing systems.[6]

Published by the IEEE Computer Society
1520-9202/18/$33.00 ©2018 IEEE

AN ILLUSTRATION: CYBERSECURITY IN SMALL AND MEDIUM-SIZED ENTERPRISES

Many small and medium-sized enterprises (SMEs) don't allocate sufficient time, resources, and efforts to secure their IT systems. They tend to think that cybersecurity investments involve high costs and low benefits. Surveys have reported that SMEs often believe they have no data of interest to cyberattackers.[7] Unfortunately, this view is often misguided and associated with a lack of true understanding of the evolving nature of cyberthreats.

According to a 2017 study by the insurance company Zurich, 875,000 SMEs in the UK faced at least one cyberattack over the past 12 months, 10 percent of which reported losses over $70,000.[8] Likewise, according to the National Cyber Security Alliance, one in three small businesses in the US become cybercrime victims every year and 60 percent of them will close within six months of experiencing a cyberattack.[9]

Poor Cybersecurity Orientation among SMEs

Despite these problems, increasing the level of preparedness to defend themselves against cyberattacks has not been a major priority for most SMEs. Experian's annual data breach preparedness study found that 45 percent of SMEs across the UK have no contingency plan in place to deal with a potential data breach.[10] A survey of more than 1,000 SMEs in the UK indicated that about half planned to spend about $1,000 on cybersecurity annually.[8] According to the National Cyber Security Alliance, 87 percent of small businesses in the US had no formal cybersecurity plans.[9]

Many SMEs tend to believe that investments in employee cybersecurity training and awareness activities will have a low return on investment. Surveys and anecdotal evidence indicate that SMEs lack initiatives to provide adequate training and support to enhance their employees' cybersecurity competence. According to a 2011 survey conducted by Zogby International, 77 percent of US small businesses lacked a formal written cybersecurity policy for employees and 49 percent lacked even an informal policy. The survey also found that 45 percent of small businesses provided no cybersecurity training to employees. Moreover, 56 percent lacked Internet usage policies to clarify websites and web services that employees can use.[11]

Similar findings have emerged from studies of SMEs in other industrialized countries. According to a survey conducted among SMEs in the UK manufacturing sector, 46 percent of manufacturers failed to increase their investment in cybersecurity over the past two years, and one-fifth failed to make their employees aware of cyber risks. Only 56 percent of the respondents said that cybersecurity was given serious attention by their board, and 36 percent had an incident response plan in place.[12]

These findings are of concern and have important implications for SMEs' cyber-defense capabilities, especially because recent studies have suggested that 40 percent of SMEs experienced a security breach resulting from employee visits to malware-hosted websites.[13]

Poor cybersecurity orientation among SMEs can be mainly attributed to the perceived high costs of cyber-defense measures and the relative newness of cyberthreats. According to the UK government's Cyber Streetwise campaign (www.cyberstreetwise.com), which aims to change how cybersecurity is viewed, a quarter of UK SMEs reported that cybersecurity is too expensive to implement. The survey also found that a fifth of the respondents did not know "where to start."[14]

Many small and medium-sized enterprises (SMEs) don't allocate sufficient time, resources, and efforts to secure their IT systems.

Changing Cost-Benefit Structure for SMEs

SMEs are facing greater regulatory pressures from governments to strengthen cybersecurity, which would affect the cost-benefit calculus of cybersecurity investments. A notable example is the Department of Financial Services (DFS) in New York, which regulates banks and insurance companies in the state. New guidance issued by the DFS in December 2014 specified stricter rules in corporate governance, login security, management of third-party vendors, cybersecurity insurance, and others. The DFS asked financial sector firms to explain the processes and mechanisms used to track potential vulnerabilities at their third-party vendors and suggested that they develop more cybersecurity expertise on their boards.[15] The head of DFS also urged financial companies to invest in cyber insurance.

Regulators are using not only sticks but carrots as well. For example, in 2015, the UK government announced a cybersecurity innovation voucher scheme that offers micro, small, and medium-sized businesses money for specialist advice to strengthen their cybersecurity.[16]

Some governments are taking measures to strengthen SMEs' cybersecurity. For instance, in the UK, Cyber Essentials (www.cyberstreetwise.com/cyberessentials) requires an organization to complete a self-assessment questionnaire, and the responses are reviewed independently by an external certifying body. This program was developed as part of the UK's National Cyber Security Program in close consultation with industry. It's been reported that most viruses, spyware, or malware found in commonly detected cyberattacks can be prevented if SMEs are Cyber Essentials certified.[17] Since October 2014, any UK government tenders are required to hold Cyber Essentials accreditation.[18]

There's an increasing tendency among organizations to evaluate the cybersecurity practices of value-delivery networks such as distribution channels and supply-chain partners. The goal is to make sure that supply-chain partners have at least the same cybersecurity standard that companies set for themselves with compliance mandated in contracts.[19] In a survey conducted by KPMG among the UK's procurement managers at large organizations across several sectors, 94 percent of respondents said that suppliers' cybersecurity standards were important when awarding contracts to SMEs. Seventy percent of the respondents were of the view that SMEs could do more to protect valuable data, and 86 percent noted that SME suppliers that suffer a data breach would be removed. Two-thirds of the responding organizations asked their suppliers to demonstrate accreditations such as Cyber Essentials or the Payment Card Industry Data Security Standard (PCI DSS).

In addition, SMEs are facing more demanding customers that place high importance on business partner companies' cybersecurity measures. It was reported that about a quarter of medium-sized businesses in the UK had been asked by a current or prospective customer about their cybersecurity measures.[8] Likewise, in a 2014 survey conducted among US adults by Princeton Survey Research Associates International, 45 percent of respondents with credit or debit cards indicated that they would "definitely or probably avoid" retailers that experienced a data breach.[20]

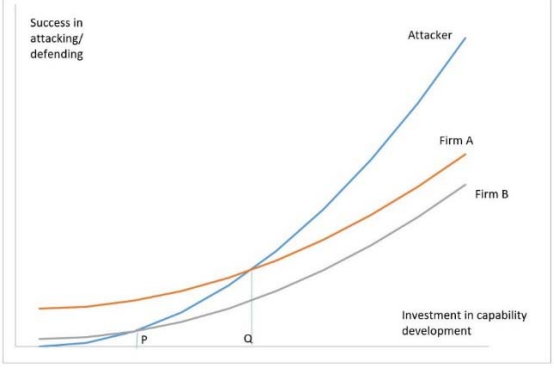

Figure 1. Development of technological capabilities to successfully attack and defend.

Finally, an additional mechanism that might force SMEs to strengthen cybersecurity measures is the rank effect.[21] The idea here is that the deployment of cyber-defense mechanisms tends to diffuse from large to small organizations. As large companies develop stronger defense mechanisms against cyberattacks, SMEs are more likely to become cyberattack targets. This is illustrated in Figure 1, where Firm A is a large firm and Firm B is a small firm.

The asymmetric nature of cyberattacks means that entities with limited financial and technical resources can compromise high-value targets. This means that the attacker is likely to have a dramatically higher success probability compared to the two firms' probabilities of defending themselves.

An implication of the rank effect is that the level of threats faced by a firm is also a function of cybersecurity measures taken by other firms. In Figure 1, both Firm A and Firm B increase cybersecurity investments over time, but at any point Firm A invests more resources than Firm B. Between time P and time Q, while Firm A's cybersecurity investment might be sufficient to defend itself from the attacker, Firm B might not be able to do so.

CONCLUSION

It's critical for SMEs to consider the rapidly changing nature of the cost-benefit structure associated with strengthening cybersecurity. SMEs must proactively track new cyberthreats and develop formal and informal policies to deal with them. They must provide information, guidance, education, and training to employees about cybersecurity. Overall, SMEs need to do more on the cybersecurity front than just complying with the demands of external stakeholders such as regulators, certification agencies, supply-chain partners, and customers.

I would love to consider your contribution in this department along the above-mentioned lines. The requirements for *IT Pro* columns in terms of length, format, writing style, and other criteria have been discussed in this issue (see "Introducing the Internet of Things Department"). Please feel free to contact me with your ideas, thoughts, and questions.

REFERENCES

1. N. Kshetri, "Economics of Linux Adoption in Developing Countries," *IEEE Software*, vol. 21, no. 1, 2004, pp. 74–81.
2. N. Kshetri, "The Economics of the Internet of Things in the Global South," *Third World Quarterly*, vol. 38, no. 2, 2017, pp. 311–339.
3. N. Kshetri, "The Economics of Click Fraud," *IEEE Security & Privacy*, vol. 8, no. 3, 2010, pp. 45–53.
4. W.B. Arthur, "Increasing Returns and the New World of Business," *Harvard Business Rev.*, vol. 74, no. 4, 1996, pp. 100–109.
5. N. Kshetri, "Positive Externality, Increasing Returns and the Rise in Cybercrimes," *Comm. ACM*, vol. 52, no. 12, 2009, pp. 141–144.
6. N. Kshetri, "Increasing Returns and the Diffusion of Linux in China," *IT Professional*, vol. 9, no. 6, 2007, pp. 24–29.
7. W. Ashford, "SMEs Believe They Are Immune to Cyber Attack," *Computer Weekly*, blog, 2014; www.computerweekly.com/news/2240216202/SMEs-believes-it-is-immune-to-cyber-attack-study-shows.
8. J. Cox, "Small and Medium-Sized Businesses Are Not Investing in Cyber Protection Despite Spate of Attacks," *Independent*, blog, 2017; www.independent.co.uk/news/business/news/sme-cyber-protection-attacks-hackers-small-businesses-medium-sized-security-online-wannacry-a7868426.html.
9. "America's Small Businesses Must Take Online Security More Seriously," *Nextgov*, blog, 2012; www.nextgov.com/media/gbc/docs/pdfs_edit/050317jm1.pdf.
10. "Almost Half of UK SMEs Unprepared for Cyber Attacks," *Nimbus CS*, blog, 2016; www.nimbuscs.com/news/almost-half-of-uk-smes-unprepared-for-cyber-attacks.

11. *2011 National Small Business Study*, report, National Cyber Security Alliance, 2011; staysafeonline.org/wp-content/uploads/2017/09/2011-NCSA-Symantec-Small-Business-Study.pdf.
12. D. Correa, "British Manufacturers Urged to Step Up Their Cybersecurity Plans," *SC Media*, blog, 2016; www.scmagazineuk.com/british-manufacturers-urged-to-step-up-their-cyber-security-plans/article/531851.
13. "GFI Labs Reports on Cybercriminals Exploiting Search Engine Ads and User Inexperience," *TMC News*, blog, 2011; www.tmcnet.com/usubmit/2011/11/11/5922728.htm.
14. E. Anderson, "SMEs Failing to Guard against Cyber Attacks, Government Warns," *The Telegraph*, blog, 2015; www.telegraph.co.uk/finance/businessclub/11430701/SMEs-failing-to-guard-against-cyber-attacks-Government-warns.html.
15. T. Kopan, "N.Y. Financial Chief Eyes Cybersecurity—Scoop: Rockefeller Wants Answers from Whisper—Energy Sector a Cautionary Tale on Cyber Regulation," *Politico*, blog, 2014; www.politico.com/tipsheets/morning-cybersecurity/2014/10/ny-financial-chief-eyes-cybersecurity-scoop-rockefeller-wants-answers-from-whisper-energy-sector-a-cautionary-tale-on-cyber-regulation-212543.
16. "New £5000 Government Grant for Small Businesses to Boost Cyber Security," *Gov.UK*, blog, 2015; www.gov.uk/government/news/new-5000-government-grant-for-small-businesses-to-boost-cyber-security.
17. R. Klahr et al., *Cyber Security Breaches Survey 2016*, report, Ipsos MORI Social Research Institute and University of Portsmouth, 2016; www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf.
18. J. Leydon, "UK SMEs with Weak Security Risk Procurement Exclusion—Survey," *The Register*, 2015; www.theregister.co.uk/2015/11/03/uk_sme_weak_security_procurement_exclusion.
19. "US Organisations Not Battle Ready in War Against Cybercrime," *Computer Business Rev.*, blog; www.cbronline.com/news/cybersecurity/data/us-organisations-not-battle-ready-in-war-against-cybercrime-4280918.
20. K.H. Queen, "Poll: Many Cardholders Will Avoid Stores Hit by Data Breaches," *Creditcards.com*, blog, 2014; www.creditcards.com/credit-card-news/shopping-after-breach.php.
21. G. Gotz, "Monopolistic Competition and the Diffusion of New Technology," *RAND J. Economics*, vol. 30, no. 4, 1999, pp. 679–693.

ABOUT THE AUTHOR

Nir Kshetri is a professor of management at the Bryan School of Business and Economics at the University of North Carolina at Greensboro and editor of *IT Pro*'s IT Economics department. Contact him at nbkshetr@uncg.edu.