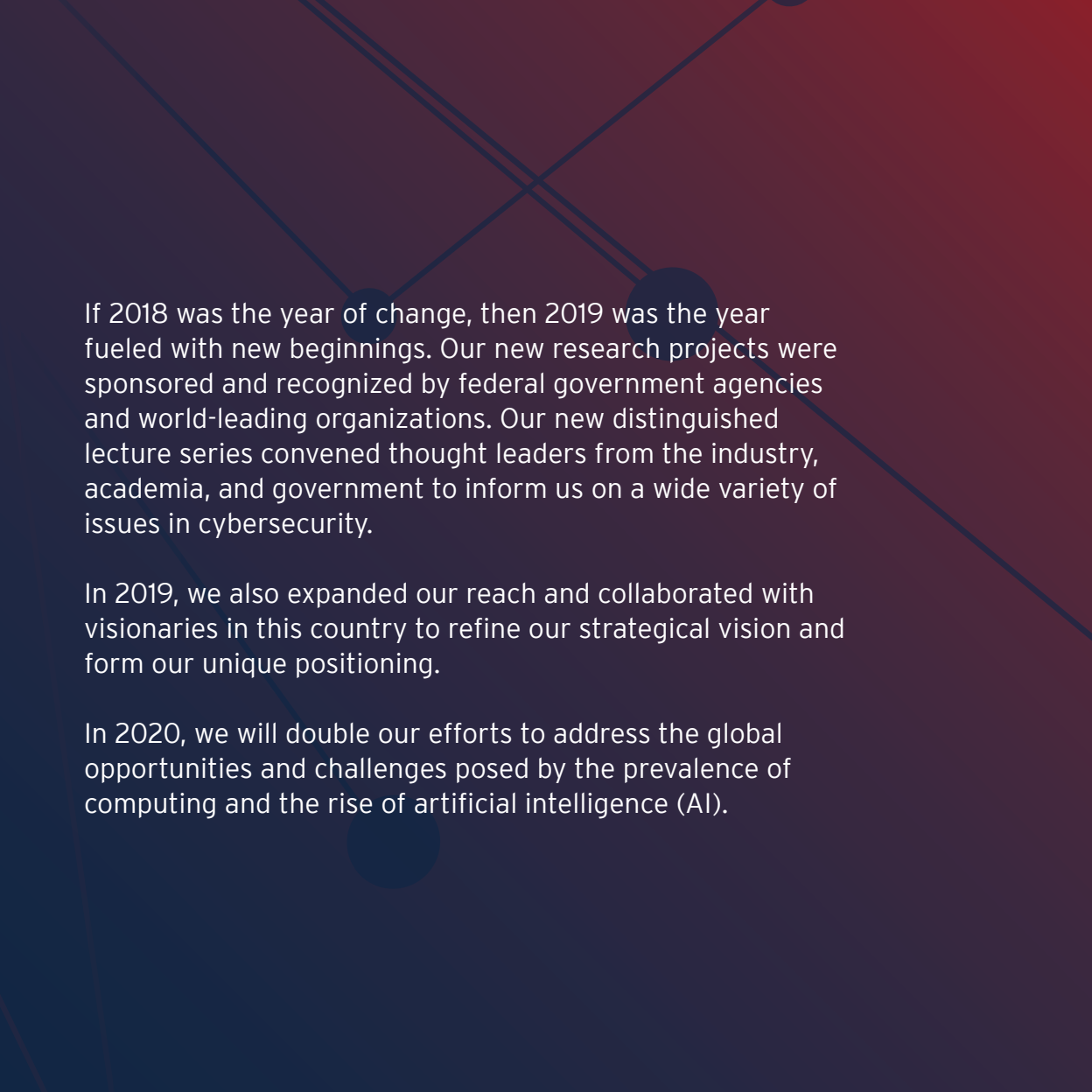




KOGOD CYBERSECURITY GOVERNANCE CENTER

Year in Review

2019 Annual Report



If 2018 was the year of change, then 2019 was the year fueled with new beginnings. Our new research projects were sponsored and recognized by federal government agencies and world-leading organizations. Our new distinguished lecture series convened thought leaders from the industry, academia, and government to inform us on a wide variety of issues in cybersecurity.

In 2019, we also expanded our reach and collaborated with visionaries in this country to refine our strategical vision and form our unique positioning.

In 2020, we will double our efforts to address the global opportunities and challenges posed by the prevalence of computing and the rise of artificial intelligence (AI).

Contents

<i>6</i>	Letter from the Director
<i>8</i>	Awards
<i>10</i>	Research Grants
<i>12</i>	Research Highlights
<i>16</i>	Expert Opinion
<i>19</i>	In the Press
<i>22</i>	Thank You

Letter from the Director

2019 was an extremely busy and productive year for us at the Kogod Cybersecurity Governance Center (KCGC)!

In the past year, we gratefully received a new research grant from the Defense Advanced Research Projects Agency (DARPA); continued our multiple projects funded by the National Science Foundation (NSF); published our high-impact research results about supply chain cybersecurity, insider threats, privacy and data anonymization; and hosted an incredible lineup of speakers at KCGC distinguished lecture series. We organized our first research roundtable to help business faculty members prepare their proposals for NSF programs in economics, management, organizational behavior, and social sciences.

At the time I am writing this letter, our nation is in the midst of the COVID-19 crisis. While the pandemic created many hardships for KCGC researchers and students, it also offered us an important lesson on the role of cybersecurity and privacy in our society. Through the public discourse on contact

tracing for COVID-19, it became abundantly clear that a broad consensus was still lacking on many key issues surrounding the ideal of responsible data practices, from the efficacy and transparency of data anonymization to the identification and accountability of algorithmic bias. It is extremely important for further research in these areas to accelerate the development and adoption of consensual standards, as evidenced by how disagreements and, sometimes, a lack of understanding on these essential issues delayed or even derailed well-intentioned efforts for combating COVID-19 in countries around the world.

To this end, I was proud to see the new initiatives from the faculty fellows of KCGC, like the launch of our Responsible AI initiative, which aims to define responsible AI governance for business through a number of research projects on algorithmic fairness, analytical transparency and accountability, and data protection. Collectively, these ongoing projects aim to develop the algorithmic techniques necessary to support

BUSINESS FOCUSED.

DATA DRIVEN.

HUMAN CENTRIC.

RISK AWARE.

the goals of fairness/transparency/privacy through all stages of data lifecycles, beginning with data collection and acquisition through cleaning, integration, analysis, and ultimately business decision-making.

So many of you were involved as collaborators, supporters, friends, and thought-partners in our journey at KCGC in 2019. In particular, I would like to welcome the newest members of our advisory board—Patricia Collins Weedon, SVP and Global CISO of Discovery Inc.; Elizabeth Petrie, director of cyber threat risk management at Citi; Mary Culnan, board VP, Future of Privacy Forum; and Allan Friedman, director of cybersecurity initiatives at Department of Commerce. I would also like to thank Michael Daly, CTO for cybersecurity and special missions at

Raytheon, for stepping up as the new chair of the KCGC advisory board. To all of you who inspired and supported us in 2019, we thank you for the meaning you brought to our work.

Here's our quick *KCGC Year in Review*—please take some time to read more about our accomplishments over the past year. We look forward to continuing collaborations and partnerships over the next year and beyond!



Heng Xu

Awards

IN 2019, KOGOD CYBERSECURITY GOVERNANCE CENTER RESEARCHERS RECEIVED SEVERAL DISTINGUISHED AWARDS AND RECOGNITIONS



2019 RESEARCH HIGHLIGHT AWARD

From ACM SIGMOD, the premier international organization for data management and data analytics researchers

Dr. Nan Zhang and his coauthors received a Research Highlight Award from the Association for Computing Machinery's Special Interest Group on Management of Data (ACM SIGMOD) for their work on "Efficient Signal Reconstruction for a Broad Range of Applications." Their work demonstrated that the efficiency of machine learning can be successfully boosted by database techniques. Their proposed solution has a substantial number of practical applications in diverse areas, including network traffic engineering, medical image reconstruction, acoustics, astronomy, and many more.

According to Dr. Zachary Ives (Adani President's Distinguished Professor and department chair of Computer and Information Science) from University of Pennsylvania, this work "is notable because it scalably addresses an underserved problem with practical impact and illustrates the potential benefits of connecting important optimization problems with database approximate query processing techniques."

LEARN MORE AT
**KOGOD.AMERICAN.EDU/
RESEARCH/CYBERGOV**



BEST PAPER AWARD 2019, CONSUMER 360° TRACK

From the American Marketing Association Academic Conference

The paper “How Much Choice is Too Much? A Machine Learning Based Meta-Analysis of Choice Overload” was co-authored by Heng Xu and Nan Zhang. It reveals new insights about the extensively studied choice overload effect by developing a novel meta-analysis method based on the recent advances of theoretical machine learning.



BEST PAPER NOMINATION 2019

From the Hawaii International Conference on System Sciences

“Protecting Privacy on Social Media: Is Consumer Privacy Self-Management Sufficient,” a paper co-authored by Yaqoub Alsarkal, Nan Zhang, and Heng Xu, won a best paper nomination from the Hawaii International Conference on System Sciences. The paper illustrates a fundamental limit of privacy self-management solutions for social media platforms—their inability to control the co-disclosure of privacy by an individual’s friends.

Research Grants

IN 2019, KCGC RECEIVED A NEW RESEARCH GRANT FROM DARPA



THEORE: Using Machine Learning to Study Human Behavior

Theory-Driven Curation and Reusable Evaluation of Research Claims in Social and Behavioral Sciences



Dr. Nan Zhang and Dr. Heng Xu got a new research grant from the Defense Advanced Research Projects Agency (DARPA). The aim of the project, under the program of SCORE (Systematizing Confidence in Open Research and Evidence), is to develop automated tools to score the confidence—or reproducibility and replicability—of scientific claims in areas such as psychology and sociology.

The overall objective is to respond to a famous quote by Senator Walter Mondale: “For every study that contains a recommendation, there is another, equally well-documented study challenging the conclusions of the first... No one seems to agree with anyone else’s approach.” The goal of this project is to demonstrate the feasibility of computationally reasoning about the robustness of various research claims based on a quantitative model that captures the connections between SBS claims, including and, especially, conflicting ones, through their shared constructs, relationships, and theories. The results of this work may help DARPA better leverage the social and behavioral sciences for insights and theories that can help address critical complex national security questions.

LEARN MORE AT
[KOGOD.AMERICAN.EDU/
RESEARCH/CYBERGOV](https://kogod.american.edu/research/cybergov)

OTHER ONGOING GRANTS

Situation-Aware Identification and Rectification of Regrettable Privacy Decisions

Funded by the National Science Foundation, 2018-2022

People today are faced with many data disclosure decisions in their daily interactions with mobile devices. Despite numerous efforts to help individuals make better privacy decisions, users still make mistakes and regret their privacy decisions. This project sponsored by NSF and directed by Heng Xu and Nan Zhang casts a fresh perspective on Privacy by ReDesign by helping users revisit and rectify past privacy decisions.

Establishing and Boosting Confidence Levels for Empirical Research Using Twitter

Funded by the National Science Foundation, 2018-2021

Concerns about a reproducibility crisis in scientific research have become increasingly prevalent within academia and to the public at large. This \$400,000 project sponsored by NSF and directed by Heng Xu and Nan Zhang examines the inconsistent handling of organic data among scholarly publications in social and behavioral sciences in order to assess the confidence (or the lack thereof) in the conclusions drawn from data analysis.

The Generalizability and Replicability of Twitter Data for Population Research

Funded by the National Science Foundation, 2018-2021

This \$500,000 project funded by NSF aims to evaluate the extent to which Twitter users represent the population across different demographic groups. Heng Xu is a co-investigator in collaboration with a group of social scientists at Penn State.

Research Highlights

A CORE MISSION OF THE KOGOD CYBERSECURITY GOVERNANCE CENTER IS TO CONDUCT WORLD-CLASS RESEARCH ON CYBERSECURITY AND PRIVACY



Jay Simon
IT & Analytics



Ayman Omar
IT & Analytics

Cybersecurity Investments in the Supply Chain

Supply chains consist of several interconnected firms that often make many decisions independently of one another. This independent decision-making presents challenges when searching for the best possible policies and investments related to cybersecurity risk management across supply chains. Senior executives are constantly trying to determine the appropriate levels of investments in cybersecurity, and most investment decisions are made in silos without taking other critical organizations in the supply chain into consideration. For example, a large retailer might invest substantial sums of money to keep customer

data protected, as the negative publicity and loss of trust associated with a breach would carry an enormous cost. However, a supplier with whom the retailer shares customer data might be less incentivized to do so, since the cost of a breach to the supplier is relatively small. In general, cyberattacks on a firm include both direct costs to that firm, as well as indirect costs to other firms in its supply chain. Improving the operational and financial performance of companies within a supply chain is only achieved when there is some level of coordination and collaboration in place, and cybersecurity investment decisions are no different. Without explicit coordination, it is very unlikely that these firms will act in a way that is optimal for the overall supply chain.

We analyze this problem using a game theory approach called an attacker-defender model, which is commonly used in counterterrorism. Each of the firms in the supply chain is a defender and must choose how much to invest in cybersecurity. The attacker observes

these investment levels and then has some probability of targeting each firm in the supply chain. We allow the attacker-defender model to vary in two specific ways: 1) whether or not the attacker is strategic, i.e. attacks specific or more appealing targets more often, and 2) whether the defenders' cybersecurity investment decisions are coordinated or made independently.

After applying this model, we observe several interesting findings: First and foremost, if attackers are not strategic (i.e. they simply attack firms randomly), then, if the firms (defenders) do not coordinate, they will systematically underinvest in cybersecurity. The benefits of a firm's cybersecurity investment on the rest of the supply chain are an example of a positive externality; other parties not involved in the investment decision are helped by it. Without coordination, externalities (positive or negative) tend to be ignored when a firm or an individual person makes decisions. Furthermore, the more interdependent the firms are, the greater the degree of underinvestment. That is, if the spillover effects on other nodes from an attack are large, then firms will underinvest substantially in cybersecurity if they do not coordinate.

We expand these results by allowing for strategic attackers, where the probability of a firm being attacked is increasing with the expected damage from an attack on that firm.

If firms act independently, strategic attackers lead to increased cybersecurity investments, counterbalancing the underinvestment observed in our first result. This occurs because when a firm invests in cybersecurity, it now receives an additional "benefit" of transferring some attack probability to other firms. For example, if the large retailer's supplier mentioned earlier is relatively unaffected by an attack on the retailer, the supplier may overinvest instead to reduce the probability of being attacked directly. However, if indirect damages to a firm are substantial relative to direct damages on the firm when attacked, the underinvestment effect persists. It is also possible that some firms will underinvest and others will overinvest.

Coordinating cybersecurity investments throughout the supply chain can eliminate these inefficient and potentially harmful outcomes and ensure an optimum level of investment that provides the most efficient use of resources across supply chain firms. Therefore, we recommend that firms develop collaborative mechanisms for coordinating their cybersecurity investments with other supply chain firms.

This study is published by *European Journal of Operational Research*: Simon, J., & Omar, A. (2020). Cybersecurity Investments in the Supply Chain: Coordination and a Strategic Attacker. *European Journal of Operational Research* 282(1), 161-171.



Gwanhoo Lee

IT & Analytics

A Chronological Review of Empirical Research on Personal Information Privacy Concerns

As concerns about personal information privacy (PIP) continue to grow, an increasing number of studies have empirically investigated the phenomenon. However, researchers are not well informed about the shift of PIP research trends with time. In particular, there is a lack of understanding of what constructs have been studied in what contexts. As a result, researchers may design their study without sufficient guidance. This problem can lead to unproductive efforts in advancing PIP research. Therefore, it is important and timely to review prior PIP research to enhance our understanding of how it has evolved. We are particularly interested in understanding the chronological changes in contexts and research constructs studied. We use a four-party PIP model suggested by prior literature as the conceptual foundation to conduct a chronological literature review of privacy studies: an individual consumer/user as first

party; a vendor as second party; a legal entity that legally collects personal information; and an illegal entity that collects or misuses personal data. We identify a fifth (hidden) party that is defined as massive multi-source data collectors/aggregators with neither first parties' notice nor consensus across the boundary of online and offline activities. We also find several PIP research trends during the last two decades, such as the quantity of PIP research has drastically increased, the variety of contexts and research constructs being studied has increased substantially, and many constructs have been studied only once while only a few have been repeatedly studied. We discuss the contributions of the study and recommendations for future research directions.

This study is published by *Information & Management*: Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, 56(4), 570-601.



Elizabeth M. Petrie

Advisory Board Member



Casey Evans

Accounting

Piloting the Exchange of Insider Threat Reports

Research published by the SWIFT Institute in August 2017 titled “Sharing Insider Threat Indicators: Examining the Potential Use of SWIFT’s Messaging Platform to Combat Cyber Fraud” proposed a protocol for sharing insider threat activities between financial institutions.

Building from the assumption that cyber criminals work off a shared services model to give them access to infrastructure, tools, targets, and options for monetizing their exploits, the research asserted the strengthening of communication channels for defenders to share real-time threat information is essential to preempting cyber fraud. A pilot to test this information sharing protocol through the development of an Insider Threat Report (ITR) message type was initiated in late September 2017. The pilot ran for 12 months, during which time participants from financial and investment services firms worked together to validate a set of insider threat indicators based on actual use cases

VIEW MORE AT
[KOGOD.AMERICAN.EDU/
RESEARCH/CYBERGOV](https://kogod.american.edu/research/cybergov)

from internal investigations and customized the ITR fields for transmitting the information over the SWIFT messaging platform. The pilot concluded with a number of findings on key challenges to this level of information sharing that, until resolved, will prevent member organizations from formalizing their engagement on this effort.

For example, the pilot highlighted the need for a common lexicon for standardizing the classification of threats so when threats are reported, a comparison can be made with internal case information to see if there are similarities. The pilot also identified cultural, legal, and regulatory considerations around sharing information, and the cultural norms were found to be as important as the legal and regulatory restrictions.

This stream of research has produced two cybersecurity grants awarded by the SWIFT Institute and one SWIFT report: Evans, C., and Petrie, M. E. (2019). Piloting the Exchange of Insider Threat Reports: Information Sharing Challenges to Proactive Cyber Fraud Identification, *SWIFT Institute*.

Expert Opinion



Mary J. Culnan
Future of Privacy Forum

Avoid a Privacy Disaster

Today, data is an important asset as new and existing devices, platforms, sensors, and applications generate data at an exponential rate. To remain competitive, companies need a data strategy that makes appropriate trade-offs between offense to support business objectives and defense to minimize risks related to data use, such as a “privacy disaster.” Privacy disasters can occur when a company uses consumer data in a way that is legal but violates public norms for acceptable use. Typically, privacy disasters reflect a management failure independent of technology. Today’s companies can help themselves avoid privacy disasters by having a formal data governance program. This program has two basic elements: 1) principles to govern their information practices, such as observing fair information practices, and 2) a process to ensure compliance with the principles as operationalized. The process

should include a risk assessment of whether or not new applications are consistent with contextual norms for acceptable use. These norms reflect expectations for what information practices are acceptable in a particular context at a given point in time and, as a result, do not raise privacy concerns in that context. Uses that violate norms are often viewed as “creepy,” such as unexpected data sharing with third practices or new technology features.

A recent IDC study predicted that by 2025, 75 percent of the world’s population will interact with data every day and that each connected person will have at least one data interaction every 18 seconds. It is unlikely that consumers will understand fully the new forms of data being collected, with whom their data is shared, and how the data is subsequently used. It will also take time for shared norms to evolve about which new practices are appropriate, suggesting that privacy disasters will continue to pose a risk for organizations. Having a comprehensive data governance program focusing on respect for customer expectations can help avoid privacy disasters and allow organizations to capitalize on the opportunities provided by new sources of data and new analytic tools.



John Brady

FINRA

COVID-19 and Cyber Risk Governance

The 2020 pandemic exposed businesses to unexpected risks without an opportunity to plan in advance. Lockdowns disrupted retail operations, closed offices, and sent staff off to access work systems and data from home. Attackers pounced on the opportunities these disruptions presented by disrupting virtual meetings, crafting phishing messages to look like CDC and government health agency updates, deploying malware targeted at the weaknesses of remote work, and many other attack methods. Unlike the novel coronavirus, however, the cyber attack methods employed during the pandemic aren't new, just recycled with a coronavirus twist in hopes of finding additional victims. And businesses that had effective cyber risk governance in place before SARS-CoV-2 were able to quickly adjust policies and tools to transition smoothly to a secure remote virtual work environment without suffering an increased rate of security incidents.

Research Pillars



CYBERSECURITY + HUMAN FACTORS

How to address the complexity and nuances of human behavior in the design of cybersecurity solutions?



CYBERSECURITY + DATA ANALYTICS

How to leverage data analytics techniques without making them a new attack vector?



CYBERSECURITY + SOCIAL EQUITY

Detecting disparities requires access to data about the minority population. Is privacy disparity a new threat?



PRIVACY + BUSINESS DYNAMICS

Who is the next Cambridge Analytica? Why is the public outraged by some data misuse but indifferent to others?



Heng Xu speaking at Georgetown University's OWNIT 2019 conference, with Simone Petrella and Amie Stepanovich



Heng Xu with the 2019 ACM SIGMIS Best Dissertation winners



Nan Zhang speaking at the 2019 Annual Conference of the Society for Industrial and Organizational Psychology (SIOP)



Heng Xu giving an invited talk about privacy research at School of Business, George Washington University



Heng Xu speaking about cybersecurity research at Embassy of Italy's cybersecurity day event



Nan Zhang speaking at AU's inaugural Winter Academy Luncheon

In the Press

2019 SANS Security Awareness Report

July 2019

Continuing collaborations with the SANS Institute, KCGC provided all data analysis support for this annual data-driven report on the state of the security awareness program in the US and beyond.

IMPORTANCE TO KOGOD STUDENTS

This year's report calls for more non-technical talents with strong communications and marketing skills to join the cybersecurity workforce (see page 21, "those most familiar with the technologies often suffer from a condition referred to as the 'Curse of Knowledge'"). This refers to a cognitive bias and means that the more expertise a person has on a subject, the more difficult it can be for them to teach or communicate about it. Security professionals often perceive security, especially security awareness, as being "simple" because it and the related technology are a part of their day-to-day life. Experts can make assumptions that security and technology are "common knowledge"

for everyone else, and they then often build their awareness program based on these misconceptions. As a result, what experts tend to communicate might not align with what non-experts need to comprehend and apply. Therefore, strong communications and marketing skills are a critical component to improve the effectiveness of an awareness program. Yet a majority (80 percent) of current security awareness professionals come from technical background; less than 20 percent have a non-technical background such as communications, marketing, or human resources. This result suggests potential cybersecurity career paths for Kogod students to consider.

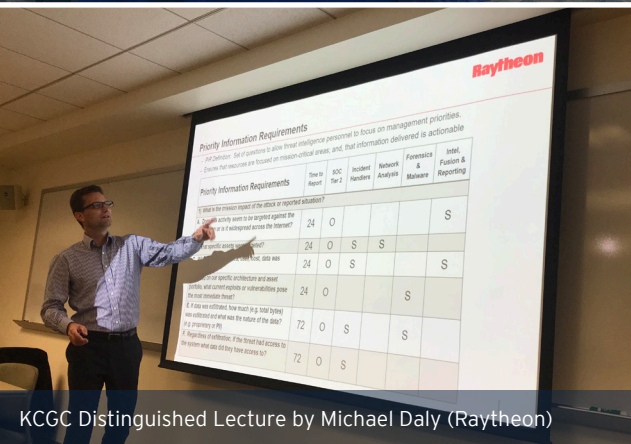




KCGC research forum



KCGC Distinguished Lecture by Allan Friedman (Department of Commerce)



KCGC Distinguished Lecture by Michael Daly (Raytheon)



KCGC Distinguished Lecture by John Brady (FINRA)



Lance Spitzner (SANS Institute)'s KCGC visit



KCGC Distinguished Lecture by Kevin Kirst (Charles River Associates)

KCGC DISTINGUISHED LECTURE SERIES

Started in February 2019

KCGC started its all-new distinguished lecture series in fall 2019 with the theme “bridging research and practice.” Since the inauguration of the series, renowned researchers and practitioners from academia, industry, and government have shared with Kogod researchers and students their insights on problems and challenges across the broad domain of information security and privacy.

2019 SPEAKERS

(alphabetical order)

John Brady, *FINRA*

Michael Daly, *Raytheon*

Sauvik Das, *Georgia Tech*

Allan Friedman, *Department of Commerce*

Kevin Kirst, *Charles River Associates*

Sasha Romanosky, *RAND*



NEW COURSE: CYBER ANALYTICS

Dr. Nan Zhang offered the new course Cybersecurity Analytics in fall 2019. The course covers a variety of analytics techniques for cybersecurity applications—from data collection and management to machine learning and visualization—and discusses their roles in strengthening the defense of critical cyber assets in today’s cybersecurity landscape.



ROUNDTABLE: RESEARCH FUNDING

The roundtable discussion was designed to help business faculty members prepare their proposals to target NSF programs in economics, management science, organizational behavior, and social sciences. Two recent NSF awardees (Nathen Larson from Economics/CAS and Heng Xu) shared their experience.



GLOBAL IMPACT: PROFESSIONAL SERVICE

Dr. Heng Xu co-chaired the 2019 ACM SIGMIS Best Dissertation competition. This competition is held annually to recognize the best dissertation research around the globe in the field of information systems.

Thank You

In order to pursue world-class research on cybersecurity and privacy, KCGC relies on the support from Kogod leadership and our sponsors.

We are very grateful for their extremely generous support, which enabled the many initiatives described in the report.

SPONSORS

National Science Foundation

DARPA

Raytheon Company

Marriott International

Discovery, Inc.

Financial Industry Regulatory Authority (FINRA)

Any opinions, findings, and conclusions or recommendations expressed in this report and any other material published by the Center or its members are those of the author(s) only and do not reflect the views of the sponsors.



KOGOD SCHOOL *of* BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC

Kogod Cybersecurity Governance Center
American University's Kogod School of Business
4400 Massachusetts Avenue, NW
Washington, DC 20016

Professor Heng Xu (director)
cybergov@american.edu
202-885-1832

