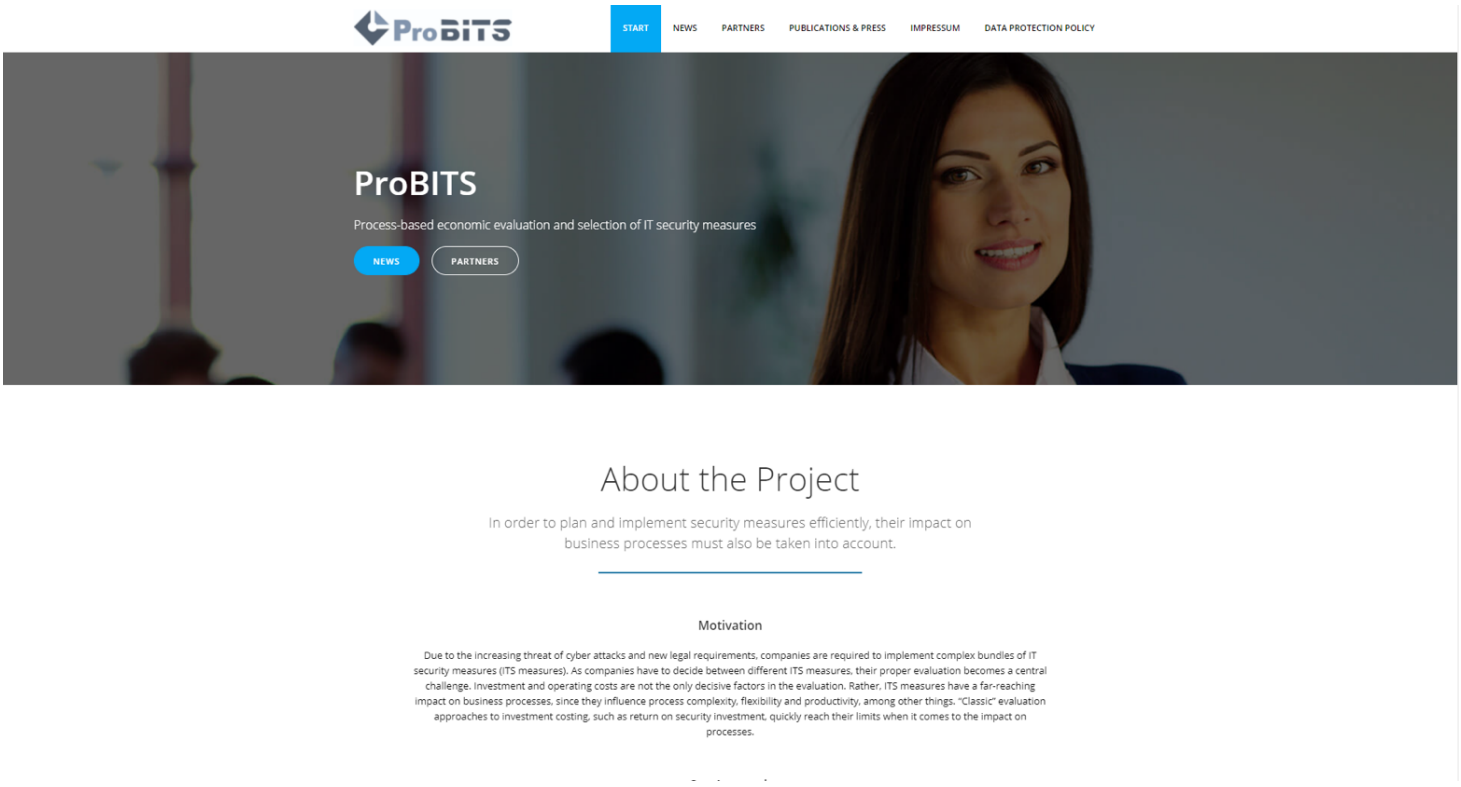
Newsletter 01 - 2021

Projektfortschritt & Aktuelles

Website ist online



Seit dem 03. Mai 2021 ist die Website des Forschungsprojekts ProBITS online. Neben allgemeinen Informationen über das Projekt, können sich hier alle Interessenten außerdem über die beteiligten Verbundpartner informieren. Seit kürzester Zeit sind nun auch unsere assoziierten Partner bekannt und aufgeführt.

Die ProBITS Website kann unter folgendem Link aufgerufen werden: https://www.probits.uni-goettingen.de/

Unter dem Reiter Publications & Press sollen Sie zukünftig ebenso auf dem Laufenden gehalten werden. Die Pressemitteilung der Universität Göttingen zum Start von ProBITS können Sie dort bereits verfolgen: **Forschungsprojekt unter Leitung der Universität Göttingen entwickelt Bewertungsmethode für Unternehmen**

Competence Center im Aufbau

Zum Wissensaustausch innerhalb des Projektvorhabens sowie für die Kommunikation mit externen Stakeholdern arbeiten wir an dem Aufbau eines IT-Security Competence Centers. Dieses soll als zentrale Instanz die Koordination und die Kommunikation des Projektes sowohl intern als auch extern steuern.

Analyse der Literatur fast abgeschlossen

Zeitgleich werden aktuell die Arbeitspakete 2 & 3 bearbeitet. Mithilfe einer Literaturanalyse sollen Grundlagen für den Entwurf des multikriteriellen Entscheidungsmodells herausgearbeitet werden. Erste Ergebnisse werden in Kürze erwartet und können im nächsten Newsletter oder auf unserer Webseite gefunden werden. Darüber hinaus sind Experteninterviews geplant um weitere Praxiseinblicke zu erlangen und relevante Anforderungen aufzunehmen.

ProBITS in der Presse

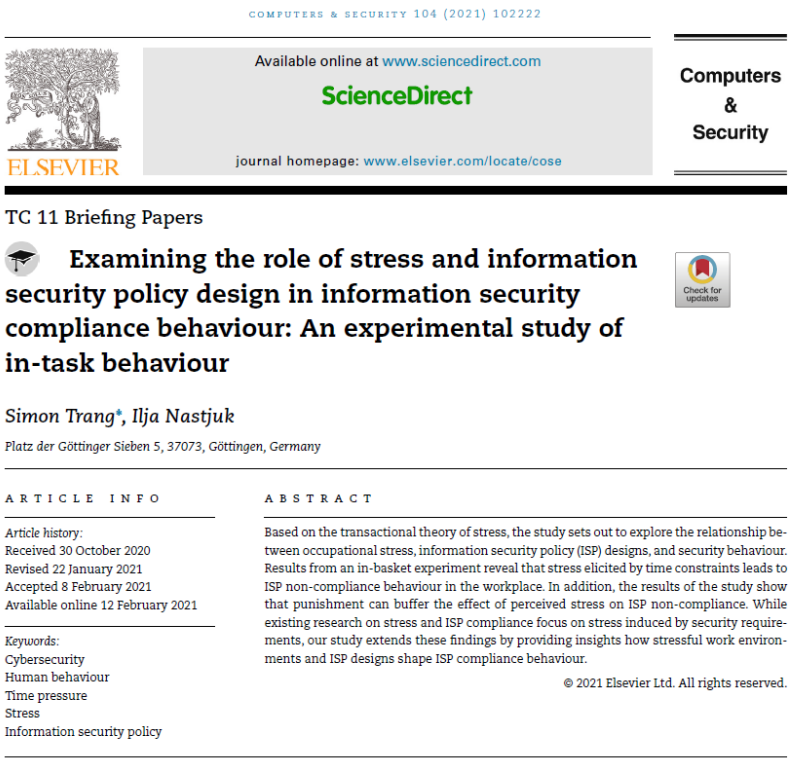
Auch in der Öffentlichkeit blieb der Projektstart nicht unbemerkt. So berichtete unter anderem das lokale „Göttinger Tageblatt“ vor einigen Wochen über das Projekt und zitierte Herrn Prof. Trang mit den Worten:

„Wir wollen die Barrieren bei der Einführung und Nutzung von ITS-Maßnahmen aufspüren und mögliche Hemmnisse abbauen. Das Projekt leistet somit einen wesentlichen Beitrag, um die IT-Sicherheit zu erhöhen und gleichzeitig ökonomische Kriterien nicht außer Acht zu lassen.“

Den vollständigen Artikel können Sie hier lesen.

Aktuelles aus der Forschung

Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. Computers & Security.



COMPUTERS & SECURITY 104 (2021) 102222

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

ELSEVIER

TC 11 Briefing Papers

Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour

Simon Trang, Ilja Nastjuk*

Platz der Göttinger Sieben 5, 37073, Göttingen, Germany

ARTICLE INFO

Article history:
Received 30 October 2020
Revised 22 January 2021
Accepted 8 February 2021
Available online 12 February 2021

Keywords:
Cybersecurity
Human behaviour
Time pressure
Stress
Information security policy

ABSTRACT

Based on the transactional theory of stress, the study sets out to explore the relationship between occupational stress, information security policy (ISP) designs, and security behaviour. Results from an in-basket experiment reveal that stress elicited by time constraints leads to ISP non-compliance behaviour in the workplace. In addition, the results of the study show that punishment can buffer the effect of perceived stress on ISP non-compliance. While existing research on stress and ISP compliance focus on stress induced by security requirements, our study extends these findings by providing insights how stressful work environments and ISP designs shape ISP compliance behaviour.

Die Wissenschaftler S. Trang und I. Nastjuk haben anhand einer Experimentalstudie den Zusammenhang zwischen der Gestaltung von IT-Sicherheitsmaßnahmen in Unternehmen, das IT-Sicherheitsverhalten von Mitarbeitern, sowie Stress am Arbeitsplatz analysiert. Die Studie baut auf bereits gewonnenen Erkenntnissen in der Stressforschung und IT-Sicherheitsforschung auf und versucht herauszufinden, inwiefern stressige Arbeitsumgebungen sowie die Gestaltung von IT-Sicherheitsmaßnahmen das Sicherheitsverhalten auf Mitarbeiterebene beeinflussen. Die Studie zeigt, dass ein stressiges Arbeitsumfeld das Sicherheitsverhalten negativ beeinflusst und Unternehmen vor neuen Herausforderungen in Bezug auf die Gestaltung von IT-Sicherheitsmaßnahmen stellt. So konnte zum Beispiel gezeigt werden, dass - im Vergleich zu Belohnungsmechanismen - angedrohte Strafen weitaus effektiver sind, um gewünschtes IT-

Sicherheitsverhalten in stressigen Arbeitsumfeldern zu erreichen.

Trang, S.; Weiger, W. (2021): The perils of gamification: Does engaging with gamified services increase users' willingness to disclose personal information?, Computers in Human Behavior

Computers in Human Behavior 116 (2021) 106644

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: http://www.elsevier.com/locate/comphumbeh

Full length article

The perils of gamification: Does engaging with gamified services increase users' willingness to disclose personal information?

Simon Trang [a,1], Welf H. Weiger [b,c,1,*]

[a] Chair of Information Security and Compliance, Faculty of Business and Economics, University of Goettingen, Platz der Goettinger Sieben 5, 37073, Goettingen, Germany
[b] Chair of Marketing Department, College of Business, Alfaisal University, P.O. Box 50927, 11533, Riyadh, Saudi Arabia
[c] Chair of Digital Marketing, Faculty of Business and Economics, University of Goettingen, Platz der Goettinger Sieben 3, 37073, Goettingen, Germany

ARTICLE INFO

Keywords:
Gamification
Gamified services
Privacy
Information disclosure
Engagement
Cognitive absorption

ABSTRACT

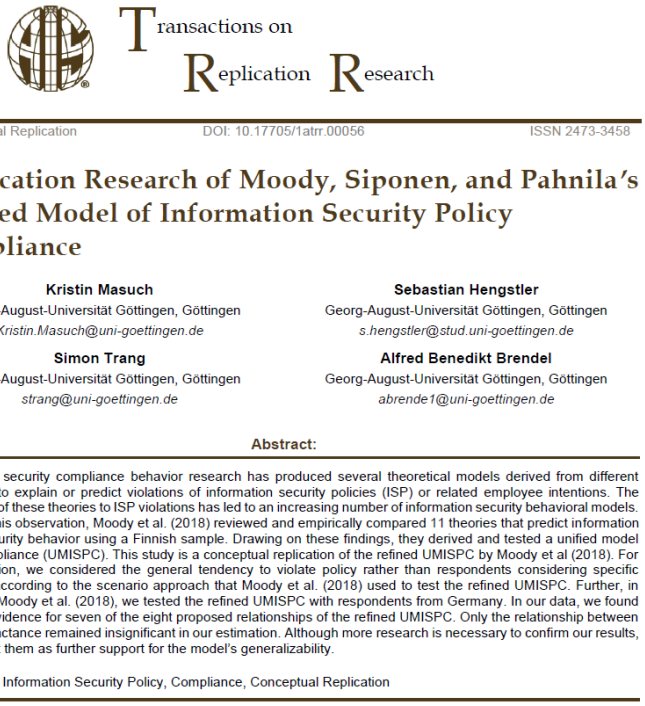
The increasing use of gamification in the digital service landscape has caught the attention of practitioners and marketers alike. Alarmingly, most of the empirical research has attested to the benefits of such gamified service (e.g. apps) use while neglecting to address potential drawbacks. This research suggests that users of gamified apps end up being more likely to share private information with firms, thus threatening their own personal information privacy. Against this background, the present study links gamification to information disclosure and demonstrates that if a gamified service conveys experiences of, for instance, social comparison, it can indeed lead to greater willingness to disclose personal information. This relationship can be explained by the users' increased resource depletion through cognitive absorption (i.e. the concentration of one's entire affective, cognitive, and physical resources on the task at hand). The results further indicate that engaging with gamified apps indeed affects the situational processing of privacy-related decisions (i.e. calculating benefits vs. risks) and the role of dispositional antecedents: In states of deep cognitive absorption, users disclose even more information when they perceive privacy benefits (i.e., situational) and even less when they have high privacy concerns (i.e., dispositional).

Empirische Untersuchungen stellen bislang größtenteils nur die Vorteile der Gamifizierung dar, lassen jedoch potenzielle Nachteile außer Acht.
In dem Paper „The Perils of Gamification" wird mittels einer groß angelegten fragebogenbasierten Feldstudie sowie einer weiteren experimentellen Studie untersucht, inwiefern Gamification die Bereitschaft zur Offenlegung personenbezogener Daten beeinflusst.

Die vorliegenden zwei Studien zeigen auf, dass gamifizierte Apps tatsächlich zu einer höheren Bereitschaft führen können, persönliche Informationen preiszugeben. Gamification induziert einen psychologischen Zustand der kognitiven Vertiefung, in dem die Nutzer so sehr auf die Aufgabe konzentriert sind, dass sie durch minimalen Aufwand im Entscheidungsprozess eher bereit sind, private Daten preiszugeben.

Die Ergebnisse dieser Studie sollen einen Nutzen für weitere Forschungsarbeiten im Bereich Gamification und Informationsweitergabe stiften.

Masuch, K., Hengstler, S., Trang, S., Brendel, A. (2020): Replication of the Unified Model of Information Security Policy Compliance, AIS Transactions on Replication Research. (Vol. 6, Paper 13, pp. 1-16)



Transactions on Replication Research

Conceptual Replication DOI: 10.17705/1atrr.00056 ISSN 2473-3458

Replication Research of Moody, Siponen, and Pahnila's Unified Model of Information Security Policy Compliance

Kristin Masuch
Georg-August-Universität Göttingen, Göttingen
Kristin.Masuch@uni-goettingen.de

Sebastian Hengstler
Georg-August-Universität Göttingen, Göttingen
s.hengstler@stud.uni-goettingen.de

Simon Trang
Georg-August-Universität Göttingen, Göttingen
strang@uni-goettingen.de

Alfred Benedikt Brendel
Georg-August-Universität Göttingen, Göttingen
abrende1@uni-goettingen.de

Abstract:

Information security compliance behavior research has produced several theoretical models derived from different disciplines to explain or predict violations of information security policies (ISP) or related employee intentions. The application of these theories to ISP violations has led to an increasing number of information security behavioral models. Based on this observation, Moody et al. (2018) reviewed and empirically compared 11 theories that predict information system security behavior using a Finnish sample. Drawing on these findings, they derived and tested a unified model of ISP compliance (UMISPC). This study is a conceptual replication of the refined UMISPC by Moody et al (2018). For the replication, we considered the general tendency to violate policy rather than respondents considering specific behaviors according to the scenario approach that Moody et al. (2018) used to test the refined UMISPC. Further, in contrast to Moody et al. (2018), we tested the refined UMISPC with respondents from Germany. In our data, we found empirical evidence for seven of the eight proposed relationships of the refined UMISPC. Only the relationship between fear and reactance remained insignificant in our estimation. Although more research is necessary to confirm our results, we interpret them as further support for the model's generalizability.

Keywords: Information Security Policy, Compliance, Conceptual Replication

In der Forschung zum Informationssicherheitsverhalten von Mitarbeitern sind im Laufe der Zeit mehrere Theorien angewendet wurden, um die Verstöße gegen die Informationssicherheitsrichtlinien (ISR) sowie die dahinterliegenden Absichten der Mitarbeitenden zu erklären oder vorherzusagen. Die Anwendung dieser Theorien hat zu einer wachsenden Zahl von Verhaltensmodellen im Bereich der Informationssicherheit geführt, von denen Moody et al. (2018) 11 Modelle als grundlegend identifizieren, um das Informationssicherheitsverhalten von Mitarbeitern vorherzusagen. Diese Modelle werden von Moody et al. (2018), anhand einer finnischen Stichprobe, überprüft und empirisch verglichen. Auf Grundlage der Ergebnisse haben sie ein einheitliches Modell, das „Unified Model of ISP Compliance“, aus den 11 Modellen abgeleitet, welches alle relevanten Konstrukte der grundlegenden Modelle beinhaltet. Die Studie von Masuch et al. 2020 setzt an diesem Ansatz an und führt eine konzeptionelle Replikation des UMISPC von Moody et al. (2018) durch. Dabei wurde ein besonderes Augenmerk auf die allgemeine Tendenz zu Richtlinienverstößen bei Mitarbeitern ergänzt und das Modell im deutschen Raum überprüft. Die Ergebnisse zeigen, dass das UMISPC auch in Deutschland anwendbar ist, jedoch die Beziehung zwischen „Fear“ und „Reactance“, anders als in Finnland, nicht bestätigt werden kann.

Kühnel, S.; Lindner, S.; Trang, S. (2019): Conceptualization, Design, and Implementation of EconBPC - A Software Artifact for the Economic Analysis of Business Process Compliance

Die Compliance von Geschäftsprozessen, welche bestimmte Anforderungen an Gesetze, Richtlinien oder Standards erfüllen müssen, haben sich zu einem starken Kostentreiber entwickelt. Sowohl technische als auch wirtschaftliche Unterstützung ist hier erforderlich. Während es auf technischer Seite bereits zahlreiche Tools zur Unterstützung gibt, wurde die wirtschaftliche Perspektive bislang eher vernachlässigt.

Ziel dieses Projekts ist die Konzeptualisierung, Gestaltung und Implementierung eines Software-Artefakts zur Verbesserung der Entscheidungsqualität und Reduzierung des kognitiven Aufwands. Auf Basis der fünf abgeleiteten Designprinzipien (DP) soll das Software-Artefakt EconBPC implementiert werden. Die Bewertung

der fünf DP´s erfolgt im Hinblick auf Verständlichkeit, Nachvollziehbarkeit, Nützlichkeit und Praktikabilität sowohl im Rahmen einer Expertenbefragung als auch mittels der Thinking-Aloud-Methode.

Die Ergebnisse zeigen, dass EconBPC intuitiv bedienbar ist. Die automatische Pfadidentifikation und die Bewertung prozessbasierter Compliance-Maßnahmen werden als kognitive Entlastung empfunden. Darüber hinaus wurde festgestellt, dass eine übersichtliche Darstellung von Ineffizienzen und wirtschaftlichen Ergebnissen zur Entscheidungsunterstützung beiträgt und eine Verbesserung der Entscheidungsqualität ermöglichen kann.

Somit können Praktiker und Wissenschaftler die Designprinzipien für die Entwicklung neuer Tools anpassen, z.B. für spezielle Anwendungsbereiche wie Datenschutz, Gesundheitswesen oder für die Automobilbranche.

Bei Fragen und Interesse an unseren Publikationen kontaktieren Sie uns gerne.

Kontakt aufnehmen

Aktuelle Entwicklungen im Bereich Informationssicherheit

IT-Sicherheitsgesetz 2.0

Bereits im vergangenen Mai wurde das neue „Zweite […] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetzt 2.0) durch den Bundestag verabschiedet und durch die Unterzeichnung durch den Bundespräsidenten in Kraft gesetzt.

Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde damit ein klares und dringendes Update der Informationssicherheit in Deutschland vollzogen. Das BSI wird durch das Gesetz in den folgenden Punkten gestärkt:

- Erfassung und Abwehr
- Cyber-Sicherheit in den Mobilfunknetzen
- Verbraucherschutz
- Sicherheit für Unternehmen

- Nationale Behörden

Doch nicht nur für das BSI gibt es neue Kompetenzen. Auch Unternehmen insbesondere die Betreiber “Kritische Infrastrukturen” (Kritis) haben einige neue Aspekte zu betrachten.

- Geldbußen werden im Strafrahmen von 100.000€ auf 20.000.000€ oder 4% des gesamten weltweiten Unternehmensumsatzes angehoben und damit an die EU-DSGVO angeglichen
- „Entsorgung von Siedlungsabfällen“ wird in die Liste der kritischen Sektoren aufgenommen
- Neue Kategorie „Unternehmen im besonderen öffentlichen Interesse“ (UNBÖFI), hierzu gehören Rüstungshersteller, Unternehmen von wesentlicher volkswirtschaftlicher Bedeutung und deren Zulieferer, wenn diese von wesentlicher Bedeutung sind & Unternehmen die mit Gefahrstoffen arbeiten
- IT-Produkte wurden in die Liste der KRITIS-Anlagen aufgenommen, der Einsatz dieser kann durch das BSI sogar verboten werden
- Die Angriffserkennungspflicht, die Meldepflicht und die Registrierungspflicht werden erweitert
- Einige Schwellenwerte wurden abgesenkt und neue wurden definiert, sodass mehr Unternehmen betroffen sind
- Es wurde eine neue Zertifizierung durch das BSI und ein neues freiwilliges Gütesiegel geschaffen

Eine intensive Auseinandersetzung mit dem neuen Gesetz ist daher für alle zu empfehlen, die bereits durch das alte IT-SIG betroffen sind oder den Verdacht haben jetzt betroffen zu sein.
Erfahren Sie mehr…

Milliardenschäden durch Cyberangriffe

Im August veröffentlichte der Branchenverband Bitkom eine neue Studie zu Cyberattacken auf deutsche Unternehmen. „Niemand kann sich wegducken“ schlussfolgert Bitkom-Präsident Achim Berg. Laut Studienergebnissen sind 88% der Unternehmen von Cyberangriffen betroffen. Die restlichen 12% sind vermutlich betroffen. Eine ordentliche Steigerung, wenn man berücksichtigt, dass es 2019 75% betroffene und 13% vermutlich betroffene Unternehmen gab. Im gleichen Zeitraum hat sich außerdem die Schadenssumme durch Cyberangriffe von 102,9 Mrd. € auf 223,5 Mrd. € mehr als verdoppelt.

Komplette Wirtschaft betroffen: Milliardenschäden durch Cyberangriffe | tagesschau.de

---

Ausblick und kommende Termine

Nächste Projektschritte

In der kommenden Zeit arbeitet das Projektteam an der Auswertung des aktuellen Stands der Wissenschaft und Praxis in Bezug auf Prozesseinflussgrößen von IT-Sicherheitsmaßnahmen sowie relevante kosten- und nutzenbasierte Bewertungsdimensionen. Diese sollen als Grundlage für den nächsten Meilenstein - der Entwicklung des prozessbasierten, multikriteriellen Entscheidungsmodells - dienen. Zu diesem Zweck werden als nächstes Interviews mit den Expert:innen der Projektpartner durchgeführt. Der Abschluss dieser Arbeiten ist für November 2021 geplant.

Kommende Termine

- **20.10 - 22.10: ISACA Conference Europe**

  Der Berufsverband der IT-Revisoren, Wirtschaftsprüfer sowie Experten der Informationssicherheit und IT-Governance - ISACA - hält seine jährliche Europa Konferenz vom 20.10 bis zum 22.10 erneut digital ab. Motto diesesmal : **Engage. Empower. Evolve.**