International Journal of Information Systems and Project Management

Volume 3 | Number 3 Article 2

2015

# Addressing consumerization of IT risks with nudging

Iryna Yevseyeva
*Newcastle University*

James Turland
*Newcastle University*

Charles Morisset
*Newcastle University*

Lynne Coventry
*Northumbria University*

International Journal of
Information Systems and Project Management
ISSN (print):2182-7796, ISSN (online):2182-7788, ISSN (cd-rom):2182-780X
*Available online at www.sciencesphere.org/ijispm*

# Addressing consumerization of IT risks with nudging

**Iryna Yevseyeva** [a]
www.shortbio.net/iryna.yevseyeva@newcastle.ac.uk

**James Turland** [a]
www.shortbio.net/james.turland@newcastle.ac.uk

**Charles Morisset** [a]
www.shortbio.net/charles.morisset@newcastle.ac.uk

**Lynne Coventry** [b]
www.shortbio.net/lynne.coventry@northumbria.ac.uk

**Thomas Groß** [a]
www.shortbio.net/thomas.gross@newcastle.ac.uk

**Christopher Laing** [c]
www.shortbio.net/christopher.laing@northumbria.ac.uk

**Aad van Moorsel** [a]
www.shortbio.net/aad.vanmoorsel@newcastle.ac.uk

[a] Centre for Cybercrime and Computer Security
School of Computing Science, Newcastle University,
Newcastle-Upon-Tyne, NE1 7RU
United Kingdom

[b] Psychology and Communication Technology Laboratory
School of Health & Life Sciences, Northumbria University, Newcastle-upon-Tyne, NE1 8ST
United Kingdom

[c] Faculty of Engineering and Environment
Department of Computer Science, Northumbria University, Newcastle-upon-Tyne, NE1 8ST
United Kingdom

**Abstract:**
In this work we address the main issues of Information Technology (IT) consumerization that are related to security risks, and vulnerabilities of devices used within Bring Your Own Device (BYOD) strategy in particular. We propose a 'soft' mitigation strategy for user actions based on nudging, widely applied to health and social behavior influence. In particular, we propose a complementary, less strict, more flexible Information Security policies, based on risk assessment of device vulnerabilities and threats to corporate data and devices, combined with a strategy of influencing security behavior by nudging. We argue that nudging, by taking into account the context of the decision-making environment, and the fact that the employee may be in better position to make a more appropriate decision, may be more suitable than strict policies in situations of uncertainty of security-related decisions. Several examples of nudging are considered for different tested and potential scenarios in security context.

**Keywords:**
consumerization; security; risks; mitigation strategies; nudging.

**DOI:** 10.12821/ijispm030301

**Manuscript received:** 30 September 2014
**Manuscript accepted:** 9 March 2015

## 1. Introduction to the consumerization of IT

Globalization and the worldwide availability of the Internet (for both stationary and mobile devices) has led to the reduction of spatial restrictions within traditional working environments, and thereby enabling the working environment to be highly mobile. Increasingly, people work not from a single office, but from multiple offices, on customer sites, when traveling, at home and in public places. At the same time, the technology markets fuel and adapt to such dynamic environments by regularly supplying a variety of new mobile devices to meet different business requirements and purposes.

The rapid development of Information Technology (IT) products and their constantly reducing costs make the best 'high-tech' technologies available not only to large companies, but also to the general public for personal usage. Data interchange between devices is also increasing. Storing data on individual devices not only becomes impractical, but also insufficient for its distributed usage. Cloud-based solutions are therefore of high demand for both private and work-related usage by employees.

This orientation of products and services towards users is known as *consumerization of IT*. Here, a user (an employee of a company) is also a consumer of devices and services, both owned by the company (the user's employer) and privately purchased by the user. The use of such products and services via the Internet for personal activities (e.g. social networks and other web tools) pushes companies to adapt business technologies and practices to allow employees access for personal purposes. At the same time, companies expect an employee to be productive and responsive at anytime from anywhere, thus removing the boundary between an employee's personal life and work. In turn, companies that keep pace with new technologies and take full advantage of them have more opportunities to improve their business and achieve both short- and long-term returns [1].

Under the conditions of a fast growing economy and improved technologies, such "mobilization" of businesses will continue. To stay competitive in such a dynamic market, companies need to quickly adapt to these trends and provide their employees with ways of working in such mobile environments, for instance by providing them with up-to-date mobile phones, laptops and/or tablets. However, frequently updating the equipment of employees is costly for companies and the pace of upgrades may not keep up with their expectations.

In such circumstances, a recent trend is for companies, large firms and *small to medium enterprises* (SMEs) alike, to allow their employees to work with their own devices. This strategy, known as *bring your own device* (BYOD), introduces flexibility for employees and affords the opportunity for the companies to satisfy the wishes of their employees to work with their preferred devices without increasing equipment budgets.

Many practitioners consider further IT consumerization inevitable. Trend Micro Inc. performed a survey confirming that 74% of IT enterprises were allowing BYOD for their employees. However, they emphasized that consumerization of IT carries strategic and operational challenges and *'creates security risk, financial exposure and a management nightmare for IT*' if not properly managed [2].

In addition to opportunities, consumerization of IT also introduces some severe security risks. These risks include: weak control over employees private devices (e.g., old or absent anti-virus software); possible weakness of protection measures of services used to transfer or store company data; potentially unsecured environments, in which employees may use their mobile devices (e.g., public places or foreign countries).

In addition to preoccupations related to technical security aspects, human factors are of high importance in the context of global consumerization. When using personal devices for work (or company devices for personal purposes), the boundary between personal and company data becomes blurred. However, attempts from companies to take control over personal devices for their better protection may meet opposition from employees, and disturb their ownership perception associated with their devices and privacy intrusion sentiments. Therefore, companies must consider these facts when developing their security policies.

In this work we consider how changes in the employees working context (from the office to public places or home) and in the ownership of the devices (from corporate to personal) introduce uncertainty in security decisions. We suggest a 'soft' strategy to assist in security decision-making under uncertainty, based on nudging. This approach has been used to create health [3] and social solutions [4] and recently studied in the context of security and privacy decision-making [5]-[12]. In particular, we consider when nudging may be beneficial to both the company and employee and, consequently, lead to a more secure and productive society in general.

In Section 2, we discuss practical approaches to risk assessment and mitigation of consumerization risks from the literature. In Section 3 we analyze in more detail the uncertainty that consumerization of IT brings to security decisions. In Section 4 we discuss risks that the BYOD strategy introduces and different levels of controls for managing those risks. We provide an approach to influencing the behavior of users to make more secure or more productive choices based on nudging techniques widely applied in marketing in Section 5. Finally, we conclude this work and outline directions for future research in Section 6.

## 2. Approaches to consumerization risk management

Different organizations may have different risk assessment strategies and may include in their security policy only risks specific to their activity. The European Network and Information Security Agency (ENISA), which develops security recommendations for EU countries, delivered a report that may serve as a good guideline for SMEs to perform a risk assessment [13]. According to this report, a company should identify its risk profile depending on the: size of the company; yearly revenue; data type a company is dealing with (e.g. critical personal data, such as medical information, customer data or employees data); loss of reputation and loss of customers' confidence resulting from unavailability of service. The critical assets should be identified among systems (server, laptops, workstations storage, archiving and backups), networks (routers, cabling, gateways wireless access points, network segments, etc.), people (HR, R&D, Sales and Marketing, Contractors and Third Party, Operations and Technology) and applications (ERP, Logistics, e-commerce, financial control, logistics) categories. In particular, for each asset the security requirements related to confidentiality, integrity and availability should be identified.

Depending on the company risk profile and critical assets, ENISA suggests selecting a number of organizational and asset-based controls that will become a part of a security requirements list, implemented within either physical security, system and network management, system administration tools, monitoring and auditing IT security, authentication and authorization, vulnerability management, encryption, security architecture, incident management or general staff practices [13]. The identified key security areas of the company help to shape its security efforts, in particular (i) defining and selecting requirements to be implemented within company's security policy; (ii) specifying key technical and management controls for preventing disasters and incidents; (iii) developing recovery plans and educational programs needed for staff training.

In addition to standard risk assessments, e.g. based on ENISA proposed scheme [13] or ISO/IEC 27005:2011 [14], when assessing the BYOD strategy of a company, opportunities should be considered. ENISA analyzed IT consumerization considering related costs and opportunities [15], and suggested various mitigation strategies to reduce the risks in the areas of governance, legal and regulatory issues and technical issues [16], which are related to potential losses and gains that a company may have with respect to confidentiality, integrity or availability of its assets when introducing IT consumerization. These mitigation strategies correlate with concerns related to consumerization reported by several Chief Information Security Officers (CISOs) of large enterprises interviewed by Microsoft [17], such as governance related to monitoring of personal devices, e-discovery associated with legal issues of business data stored on personal devices, and general security and control of data for privately owned devices.

MWR Security published a detailed report on mobile devices security, including BYOD strategies for companies, in cooperation with the Centre for the Protection of National Infrastructure (CPNI) [18]. According to this report, companies developing a security policy including mobile devices and BYOD strategy should consider the following challenges: (i) fast developing IT technologies in general and the constantly emerging variety of mobile devices in

particular; (ii) different risk profiles within variety of vendors of the same type of device (for instance, iPhone-based and Android-based mobile phones risk profiles are different, moreover, risks vary between devices using different versions of the same Operating System (OS)); (iii) assets that a company possesses and tries to protect; (iv) possible assets vulnerabilities (which are assets weaknesses that can be used for security breaches); (v) threats (against what the protection efforts are directed) and risks specific to the activities of the company and its employees; (vi) variety of working locations, both public (cafes, parks, hospitals, organizations) and private (home, other companies); (vii) organizational structure, whether it is an SME (with mainly 3rd party vendors/suppliers taking care of security) or a large company (with a CISO dedicated to maintaining company security).

In addition to technical challenges, attention should be paid to users' awareness of risks, their education and the provision of recommendations to users whenever possible [18]. Employers may consider different educational tools to communicate the requirements of the security policy, reasons for these requirements, benefits of compliance, and consequences of non-compliance and thus promote a security culture. However, these long-terms approaches require time and involve user awareness and conscious decision-making. While users may be aware and intend to behave securely, these intentions do not always translate into actual behavior. Therefore a complementary alternative approach would be to try to influence the behavior of the decision makers directly at the moment of the decision-making.

Influencing users behavior rather than forcing it appears to be an attractive option when security decisions are made in situations of uncertainty, when users may be required to balance competing requirements (e.g. security versus productivity), and/or when dealing with mobile devices, which employees use, but which are not fully controlled by the company-employer.

## 3. BYOD Vulnerabilities

Vulnerability can be seen as 'the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw' [30]. For the purpose of this paper we shall reflect explicitly on the first two elements assuming a 'worst case scenario' in the latter (data theft, financial loss, etc.). With this paradigm, we present an environment where there are numerous intervention methods to reduce risk and conversely several exploitations with respect to the BYOD trend. It is necessary to discuss each in light of users' behaviors.

### *3.1 A system susceptibility or flaw*

With the introduction of unknown devices into the network the likelihood of a susceptibility or flaw increases. Unknown devices are typically self-monitored and (specifically in this case) are mobile. This is highly problematic as the unknown software, mobile nature and the method in which the device is used present a real security threat. The phrase, 'a system is only as strong as its weakest link' is highly appropriate when such devices will be configured and managed manually with numerous issues associated with this.

Within many companies employees' computers are centrally managed under a specific data security policy. These machines are static often with a single user per machine and are homogenous throughout the company (with possible exceptions in policy related to specific roles within the company – i.e. installation rights, administrator access etc.). This allows for a robust, secure (albeit policy dependent) environment where risk can be mitigated by rigid control mechanisms. Installation of software can be blocked, operating system, virus scanner, firewalls and software patches can be automatically deployed and attachments to peripheral devices can be denied or monitored to name but a few.

With BYOD, however, the above level of central control is lost. Self-managed devices are typically not used in the same manner and often fulfill a multitude of roles. For example, an employee owned laptop would be used in both an office environment for work and a home environment for non-work activities. This duality of use, stronger sense of ownership, lack of knowledge, lack of prioritization of security by users and lack of central control, may lead to security features being omitted or simply not configured correctly, particularly if the security feature is perceived as inconvenient or hindering productivity. Activities that would either be impossible or forbidden by policy are now

available and this presents a conflict for users related to what they are and are not allowed to do. For instance, a given website or software may be forbidden and inaccessible on a work machine. Does this, however, mean that it is forbidden on an employees' own machines outside of work?

Unsafe practices on a personal device outside of the working environment are problematic when re-introducing a device to the work environment. The device has transformed from a personal device back to a work device but has, in the process, been exposed to numerous policy breaching activities. It is highly likely that the device has (from a company perspective) connected to unknown networks, with unknown traffic, attached to unknown physical devices (a highly relevant problem with recent documentation on USB stick firmware exploits – 'BadUSB' [31]). This presents a major threat to the company's infrastructure and data security if not carefully managed (e.g. via separate networks for personal devices).

### *3.2 Attacker access to the flaw*

Attacks generally fall into three categories [32]: persistent targeted; single targeted; or random (chance). The adoption of BYOD is vulnerable to all of these and presents an attractive avenue for attack. One could further argue that BYOD introduces an additional 'physical' attack relating to device theft that is exacerbated by the mobile nature of the device (particularly problematic if the device is not encrypted).

Targeting such a device can be beneficial to an attacker for many reasons. Firstly, it enables personal targeted attacks (i.e. targeting the CEO), which allows attackers to be much more focused. As cyber-attacks are often financially motivated (with time being a key factor) identifying such a device optimizes the attack by enabling bespoke (either physical or device specific) methods to be devised. The attacks are likely to be more successful due to the susceptibilities noted in 3.1 and the availability of the device to be attacked (predominantly in a more unsecured environment).

To understand such an attack and how BYOD may create new threat vectors, it is necessary to work through a practical example. A Man-in-the-Middle [33] attack exploits a network connection by intercepting traffic sent and received. The most successful Man-in-the-Middle attacks aim to remain anonymous by having a negligible (particularly unnoticeable by humans) impact on users' activities. Data is intercepted and subsequently analyzed in an effort to exploit a particular vulnerability (e.g. stealing Facebook login details via FireSheep FireFox plugin [34], [35]). Following the example demonstrated in [8] we see a typical BYOD scenario where attackers can exploit users' behaviors. When in a public environment the user accesses a public Wi-Fi network, the device is placed under threat. Open Wi-Fi networks present an unknown threat environment, where it is impossible to verify other users and identify malicious activity. This infrastructure provides a relatively simple platform to intercept and steal data as in the above Facebook example [34], [35] if connections are not encrypted (which is typical for small-medium enterprises and general public use). Unencrypted connections on such networks are simple to intercept enabling specifically targeted attacks to be highly successful.

Exploiting users' behaviors via phishing is also a common approach. This attack plays on users' vulnerabilities and attempts to deceive users into carrying out an action (such as clicking on a link). This is a non-technical attack, which targets users, not physical hardware or software. Phishing is a problem since permissions are often granted erroneously by users, who are fooled into believing that the task they are presented with is genuine. By providing authorization, the attacker can then gain sensitive information (often usernames and passwords) allowing them to masquerade as a genuine user. It is then extremely difficult for the system (moreover the system administrator) to determine whether or not a user is who they say they are.

### *3.3 BYOD risks and controls*

There is clearly significant impact of BYOD on a network's security infrastructure if not managed in a controlled manner. By enabling users to transport their devices between environments, new vulnerabilities and exploits are

presented that must be combatted. It is important this control is managed in a fashion that does not detract from the core attraction of BYOD, particularly mobility and productivity.

## 4. Assistance in risk assessment under uncertainty

We now propose an approach to risk assessment assistance in situations of uncertainty. The standard risk assessment procedure, for instance suggested in [13] or [14], is adjusted taking into account consumerization of IT adaptation, e.g. proposed in [16], and includes: the estimation of company activities profile; the corporate data and the evaluation of the vulnerabilities and threats of professional or personal devices; the security checks of services that employees use on a daily basis; and the analysis of potential human behavior vulnerabilities. Moreover, we consider the ownership of devices and data (private or corporate) as well as the context, in which the devices, services and data are used. Here, by context, we mean a dynamic environment, e.g. work, home or a public place, in which the mobile device users may utilize devices or data or services. Note that the context may include services that the employee is allowed to use including those owned by the company, bought by the employee or even freeware.

### *4.1 Risk assessment for consumerization of IT*

The designer of a security policy for a company working with mobile devices should consider the properties given in Table 1. Together with important functionalities, they may expose security vulnerabilities of devices. Paradoxically, one of the greatest advantages of mobile devices, mobility, is also one of its greatest vulnerabilities. Some devices (laptop and tablet) have large screens, which makes them convenient for regular tasks (e.g., writing/reading emails, programming, watching video), but it also becomes easier to shoulder surf these devices and for data shown on large screens to be disclosed accidentally. In Table 1 '+' refers to a vulnerability being present, '-' means that a vulnerability is not present and '?' refers to the presence of a vulnerability being unpredictable.

Here, we refer to a private device as a mobile device bought by an employee and to a corporate device as a mobile device bought by a company for an employee to work on. Then, a mixed-usage device is a private or corporate device used for both personal and work purposes.

Table 2 presents an example of threats adapted from [18] to mixed-usage devices, taking into account vulnerabilities presented in Table 1 and considering possible scenarios in which an employee may happen to work.

Table 1. Vulnerabilities of devices

| Property | Laptop | Tablet | Phone | USB Stick |
|---|---|---|---|---|
| Connectivity | + | + | + | + |
| Mobility | + | + | + | + |
| Applications | + | + | + | + |
| Lock | + | + | + | ? |
| Remote Access | + | + | + | + |
| Out of date software/OS | + | + | + | + |
| Large screen | + | + | - | - |
| Admin access | + | ? | ? | - |
| Removable Media | ? | + | + | - |
| Access to SIM card | ? | ? | + | - |

On the one hand, many threats presented in Table 2 can be controlled with technical solutions, such as data loss/leakage prevention (DLP), if private devices are locked down in a similar way to corporate devices with some security policy and/or with mobile device management (MDM) programs that allows management of the assets (both devices and data). Security practitioners consider MDM as a necessary risk prevention tool [19], and highlight the urgent need for an MDM version for Android-based devices [20] for companies adopting IT consumerization. Companies with 'mobile' employees already appreciate the help of mobile Virtual Private Network (VPN), which extends a private network across a public network. Research in Motion (RIM) announced a multi-platform version of its BlackBerry Enterprise Server [20] for improving the security of mobile devices. Separation of private and corporate data with data segregation tools may help to differentiate data that should be monitored from that which is personal.

Table 2. Threats for devices and corporate data

| **Device compromised** | **Device contaminated** | **Communication compromised** | **Data compromised** | **Data disclosed** | **Security/trust model weakened** |
|---|---|---|---|---|---|
| Device lost | Malicious application installed by user | Data interception in transit | Integrity (access via security breach) | Inappropriately stored / transferred data | Personal credentials shared |
| Device stolen | Device infected by malware / virus | Encryption key disclosed | Confidentiality (access via security breach) | Discloses data after being asked (social engineering) | Device jailbroken |
| Device decommissioned | Device contamination | Insecure unencrypted connection | Availability (denial of service) | Discloses data unintentionally (shoulder surfing/ duplication) | Security controls bypassed |

On the other hand, many threats presented in Table 2 involve risk prone actions, which increase security breaches significantly. Hence, companies' security policy efforts are twofold: the identification of technical controls to apply (e.g. which anti-virus to buy, which software to install and how to control its updates, allowable ways to access corporate data and how to guarantee data protection) and the prevention of possible human errors. This should be via technical controls when possible, such as control over anything installed by users and password creation rules, or with education sessions, for instance on not sharing personal credential, public Wi-Fi connection and policy jail-breaking.

Risk is usually considered as the likelihood of an attack multiplied by its impact, where the likelihood of an attack is given by the probability that a threat can exploit a particular vulnerability. A typical approach to reduce risk is therefore to add some control over the vulnerabilities, so that they are no longer exploitable. However, the usage of mixed-usage devices raises the problem of who is responsible for applying this control. Here, control refers to 'a measure that is modifying risk' [14].

Moreover, we differentiate between different levels of control that may help maximally reduce risk with: full control over devices; partial control over devices; or no control over devices. Table 3 adapted from [18] shows four possible cases of combination of a device owner and a device manager: 1) company provides employees with devices and takes full control of these devices, e.g. typical BlackBerry 'work phone'; 2) company provides devices, but does not manage them, e.g. common for universities, having partial control over the devices; 3) employees own devices are controlled by companies partially, e.g. can be registered to be wiped in case of loss; 4) employees are allowed to work with their own devices, but have to take care of security themselves, resulting in company having no control over the devices.

Table 3. Company control of devices depending on ownership and management

| | | Device Manager | |
|---|---|---|---|
| | | **Company** | **Employee** |
| **Device Owner** | **Company** | (1) Full control | (2) Partial control |
| | **Employee** | (3) Partial control | (4) No control |

The first case (1) is the case of full control: a company both owns and manages the device. Depending on how restrictive the security policy is and compliance levels, there are still possible threats and corresponding risks to the assets of the company, e.g., zero-day vulnerabilities. In case (2) a company provides devices, but does not manage them, or in case (3) employees use their own devices, and the company manages them or the company does not manage them as in case (4). In cases (2) and (3), a company may apply some security policy to protect the employee's personal or corporate devices with DLP and/or MDM tools. In case (4), there is a danger of uncontrolled threats, as an employee might not use all, or any, protection measures, such as an anti-virus, software updates, passwords, etc.

## 5. Nudging for mitigating security risks and improving productivity

A security policy should be seen as a protective measure, which employees should comply with. In addition to punishments for risky behavior and rewards for secure ones, it should take into account the employee's perspective. A highly restrictive security policy that limits flexibility for employees might result in a rebellion effect and push employees towards ignoring it. Fundamentally, such behavior would expose the company to security risks and corresponding costs that should be taken into account when developing a security policy. The problem of non-compliance with security policies has highlighted the existence of a compliance limit for each user (probably, varying from user to user) known as the "compliance budget" [21]. Further research [22] focused on understanding non-compliance and workaround strategies employees apply in order to be more productive and perform their tasks faster.

Moreover, too restrictive security policies may be insufficiently flexible to the dynamic context, in which security decisions are made. For instance, a security policy, may only allow employees to connect to Wi-Fi's in the *whitelist* of a company. However, there may be no available white-listed Wi-Fi's at the employee's current location. Hence, the employees would be unable to work if the policy is enforced on their device, or if the policy is not enforced, they may choose to breach policy and connect to a publicly available Wi-Fi. Unfortunately, at the moment of making security decisions there is often no objective information to aid the user in evaluating the consequences of each possible choice and/or the decision makers might not realize the risks and consequences of possible security breaches. However, the choices are still made (e.g. one of the Wi-Fi's should be selected for work) and the decision maker must take responsibility for the consequences of such decisions.

The traditional approach for helping employees making better security decisions is via education and training sessions about the security policy of the company [16], [18]. This is a time-consuming approach that requires conscious reflection of employees on security issues and possible consequences of such decisions for them and their company. However, awareness and knowledge does not necessarily lead to the required behavior as it does not provide cues to action, at the moment the behavior is initiated. Alternatively, nudging is an explicit recommendation or more subtle influence emphasizing some choice, but not forcing it. It has a reputation of being able to make a big difference by small changes while leaving the freedom of choice to the decision maker. This is important when security decisions are made in situations of uncertainty, where an employee might have better situational awareness than the company had when creating the policy.

### *5.2 Nudging for security and productivity: What is it?*

In this work, we investigate a possibility of applying a recently proposed 'nudging' approach [23] to influence information security choices as a 'soft' alternative to more restrictive security policy. Nudging provides a framework, called choice architecture, which presents available alternatives in such a way that influences the decision maker's final choice [23]. This approach is referred to as libertarian paternalist, in the health and social behavior domains 'people are free to do what they choose, but that it is legitimate to influence people's behavior in the positive direction' [24]. This approach has been adopted by the governments (e.g. UK and USA) to encourage behaviors promoted by government policies while still providing freedom of choice.

Nudging has been widely used in healthcare [3] and social policies [4] to change the behavior of people with minimal interventions. In these initiatives the nudged behavior is widely accepted as the 'best' by both governments and citizens, such as fighting obesity or paying the right amount of tax. The research results on applied cases of nudging are very encouraging and show that, indeed, the manner, in which the information is presented to the decision maker, influences the choice. For instance, it was shown that rearranging menu items in student's cafeteria may increase/decrease consumption of a particular item by up to 25%, since the first options in the list have higher chances of being selected [23].

Similarly, nudging can be adapted to influence people's choices in information security. The behaviors towards which nudging will direct people should be based on rigorous models developed using quantitative risk assessment techniques. They should take into account the trade-offs between productivity benefits and security risks for each particular scenario, and nudge the decision maker towards the best compromise trade-off solutions, but also taking into account context of the decision-making, security policy of the company and preferences of the particular decision maker when possible. Assuming that uncertainty is present in such security scenarios, the outcome of the rigorously assessed models will be used to frame choice architecture for decision makers in such a way that it nudges decision-makers to make the 'best' information security and productivity decisions, but still leaves the final choice for the decision maker. This assumes that the decision maker understands what is better for them in the context of the decision-making.

### *5.3 Nudging for security and productivity: How to influence?*

Six techniques are presented in [23] to support the creation of nudges: incentives, understanding mapping, defaults, give feedback, expect error and structure complex choices. They can be used to build a choice architecture that aims to influence choice made by the decision maker.

To develop incentives for information security, we need to understand the rewards that would encourage employees to make the choices we want, and the punishments that would stop them from making choices we do not want. For instance, would warning messages when connecting to a fast unsecure Wi-Fi network encourages employees to switch to a slower but more secure Wi-Fi that does not present such warnings?

To understand mappings between available options and consequences that follow, we need to be aware of the risks employees take and the convenience employees gain. For instance, studies looking at choosing between more secure Wi-Fi not protected by a password and less secure Wi-Fi protected by a password shows that people perceive more secure solutions as being more complex by default, and less secure solutions being easier and faster to implement [25].

Default choices are selected by people who 'go with the flow' and do not pay much attention to them. Default choices for security-related decisions should be pre-selected to the most secure ones, leaving the freedom for users to uncheck selections or change defaults if desired.

Giving feedback on choices, whether positive or negative, helps users to learn from their past decisions and use this experience in the future. Knowing that users make errors and expecting errors means those developers should provide choices in a simple and understandable manner, as well as guide choices with explanations and help options. They should also ensure that the user is protected against any unrecoverable decisions. One last point is also important, the

presentation and structuring of complex choices should reduce people's cognitive load, e.g., sectioning decisions so that there are clear steps and a limited number of options to choose from at any point in time [26].

In addition to the six techniques provided by choice architecture, organizational psychology and behavioral economics have identified many different factors that influence behavior. The MINDSPACE framework [27] summaries these influencing techniques some of which are common to those presented in [23]: messenger; incentives; norms; default; salience; priming; affect; commitment; and ego. Messenger effects suggest that the person delivering the message and not the message itself influences people. Norm effects suggest that people will behave in the way that those around them behave, or in ways they think people expect them to behave. Salience refers to how to present choices so that the desired choice stands out from the others and grabs the attention of the decision maker. Priming addresses framing effect, which is related to our subconscious processing of information. This is an implicit memory effect where exposure to a stimulus influences how a person responds to the next stimulus. Affect refers to people's emotional reaction to a stimulus. Commitment refers to a person's desire to keep promises they have made to another person, particularly if the commitment is written down. Ego refers to acting in a way that makes people feeling good about themselves. These factors can be used when designing choice architectures in security to optimize the chances of the nudge succeeding. In addition, [28] outlines a process by which companies can explore the creation of nudges to solve specific security problems within their companies by using MINDSPACE as part of creative workshops with staff to identify factors influencing their security behaviors within the company and to identify possible approaches of designing ways of increasing security compliance.

### *5.4 Nudging for security and productivity: When is it appropriate?*

The company may decide when to apply nudging depending on the level of control the company has over the device. Recalling Table 3 with four various cases of device ownership and management, resulting in three levels of control: full, partial and no control for the company. Taking into account the context in which the security related decisions are made, here, we argue about the appropriateness and benefit of nudging, see Table 4. Similarly to Table 3, we consider the owner and manager of the device (company or employee) and context (working or not, e.g. public places, home, private houses, other companies). In the Nudging column of Table 4, '+' indicates a situation where nudging may be desirable and '-' indicates cases, where nudging is not beneficial.

Table 4. Devices control and nudging

| # | Device Owner | Device Manager | Context | Control | Nudging |
|---|---|---|---|---|---|
| (1) | Company | Company | Working | Full | - |
| (2) | Company | Company | Public/Private | Partial | + |
| (3) | Company | Employee | Working | Partial | + |
| (4) | Company | Employee | Public/Private | Partial | + |
| (5) | Employee | Company | Working | Partial | + |
| (6) | Employee | Company | Public/Private | Partial | + |
| (7) | Employee | Employee | Working | Partial | + |
| (8) | Employee | Employee | Public/Private | No | - |

Note that in this context we can also include services that the employee is allowed to use. For instance, in the case where publicly available services are used by employees at work on working devices, such as Dropbox or social networks, the scenario should no longer be classified as the first case of full control.

Indeed, nudging is appropriate for all cases presented in Table 4 with the exception of case (1) of full control, where a company controls and manages devices and they are only used for work and case (8) of no control, where there is no control over an employee owned and managed device used in a non-work context. For instance, an Information Security policy may state that users should not access social networks from a work device. A company may restrict access to such a websites and prevent access in case (1). However, that would not be possible in case (3), where an employee is managing a corporate device, or in case (6), where an employee works on a personal device providing some managing privileges to the company, and such a restriction would disturb the employee's sense of ownership. On the contrary, nudging employees away from social network websites during working hours would be seen as advice from the company that an employee can override when justified, e.g., for working purposes in order to advertise some company products or jobs in social networks.

### *5.5 Nudging for security and productivity: Examples of tested scenarios*

Nudging has been explored in information security, for instance, for nudging users away from privacy invasive choices [5]-[8] by using color to positively and negatively frame information. Traditionally, red is associated with danger, e.g. red in traffic light or the infamous 'red button', and green with safety or 'to go' in a traffic light signal. Traffic light color schemes are widely applied in cyber security design, e.g., for indicating what can be done with shared information in a traffic light protocol [29] or for framing choice options [5].

One of the possible applications of nudging in the security context is presented in [8], [11], where a traffic light color scheme is used for a choice of public Wi-Fi. In this work an example of nudging a user towards selecting a more secure Wi-Fi is considered. Choice architecture is organized so that available Wi-Fi's are ordered in such a way that the most secure networks are placed at the top of the list and their names are colored 'green', while names of less secure Wi-Fi's are 'yellow' and open Wi-Fi's are 'red'. The results show that the color was effective in influencing the choice of users, more than the order, which did not change the choice significantly. However, in preliminary evaluations the combination of order and color was the most effective nudge, encouraging more people away from insecure networks than one factor alone.

### *5.6 Nudging for security and productivity: Examples of potential scenarios*

The following scenarios are considered as examples of scenarios where nudging can be applied efficiently, choosing a new password and determining whether to accept or decline a mobile application's permissions. In these scenarios decision makers are facing a trade-off decision of choosing between being more productive or more secure. For instance, creating a new password, which is similar to the old one, is fast and takes less time and effort to remember, however, this strategy leads to creating weak passwords according to security metrics [36]. Similarly, accepting all permissions that an application requests during installation on a mobile phone is fast and easy, however, it might compromise the user.

Regular password renewal is a common procedure used by companies to provide protection from potential malicious attackers. Many academic papers have highlighted both the need for secure passwords and how to create them [37] ('strength' meters are now commonplace). Equally important, however, is the frequency and rules that govern this process (how often passwords are updated and their complexity). It is essential to strike a balance between maintaining security and inconveniencing users. If a password is renewed too frequently then the chance of forgetting them is increased, and the users' willingness to comply decreases [38]. Forcing users to create too strong passwords may lead either to difficulties of memorizing passwords, create security breaches as a result of writing passwords down and exposing them to potentially malicious attackers or forgetting them. Alternatively, nudging may help with creating a more secure, memorable password.

At its core, a nudge should be holistic and not annoying. This is essential for password creation, as we do not want to over-burden users with additional time consuming requests or cognitive load. At the same time users should be able to override a nudge if they have strong preferences towards an option different from the one suggested by a nudge. The

nudge for password creation must be present at the point where the password is being formulated, for instance, a point immediately after requesting a user to create a new or to update an old password and before the cognitive process is started. The point of password entry is too late. The experiment described in [39] has demonstrated the direct impact of forcing users to wait a fixed time period in order to improve their password strength. Perhaps a social nudge would also be beneficial here. Social nudges work by playing on social norms. For instance, users can be informed that a high percentage of people in their company update their passwords regularly with strong alternatives, e.g. a popup is presented '74% of employees choose a stronger password than this one'.

Applications are requesting more and more permissions to access information and services on your mobile phone, for instance your personal information, your precise location, or full network access. New communication technologies such as Near Field Communication (NFC), Bluetooth LE (Low Energy) provide new methods to share data stored on given devices. These new technologies, however, are utilized by applications (e.g. NFC typically used for card payment methods and Bluetooth LE by sport fitness accessories) that must first call operating system methods that are governed explicitly by permissions. On installation of an application, these permissions are presented to users in order to detail what the application has access to and some indication of why it is necessary. Unfortunately, current implementations of this process are poor and end users have little, comprehensible information on which to base their decisions. An application may request (perhaps legitimate) access to the address book, but without direct statements regarding why such access is required, it is unclear whether or not these should be accepted. For instance, why would a torch application on a mobile phone require access to your location? The path to finding out exactly what permissions is being requested, and what they mean may well be made deliberately difficult by app developers – to nudge people to simply accepting all permissions! Recently, Facebook [40] received negative press coverage for their applications due to the way in which the permissions were presented and worded when in fact the core functionality of the applications remained the same. It was the permission text that had changed thus generating negative connotations of privacy invasion to users. Here adding more information on the usage of the requested data by the application would help in nudging users towards more selective responses.

By extending the permission text to include possible implications of accepting the permission, the user would be more informed as to whether or not they wished to accept and thus install the application. This would potentially prevent significant data leakage and personally identifiable information via uploading of contacts or media on the device for example. Similarly to the previously discussed Wi-Fi study [8], ordering and coloring could be adopted to highlight the most significant threats to security. As demonstrated in the previous study, ordering and coloring had a significant positive effect on the security of the chosen Wi-Fi network. To demonstrate, access to the address book or media could be highlighted red and given prominence by ordering it at the top of the list (with additional related text to highlight the potential impact of sharing this). Typically less security invasive permissions would conversely be ordered towards the bottom and highlighted green (permission to change the ringtone for instance). The combination of these visual nudges enforced with priming would allow users to make more informed decisions as to whether the application was indeed trustworthy or whether it was suspicious (why does a solitaire game require my location?).

Both of the above examples of potential nudges provide an interesting test bed for future investigations and highlight the complex nature in which security decisions are made. Encouraging users to make more secure decisions should not prevent them from being productive when needed and nudging appears to be an easy form for such soft influence, which can be applied together with other complementary ways of influencing users by educating and training them on a regular basis.

## 6. Conclusions

In this work, we have discussed the recent trend of both large companies and SMEs towards adopting the consumerization of IT. In addition to the commonly recognized risks and opportunities that this trend carries for the companies and their employees, we highlighted the uncertainty that consumerization introduces. This uncertainty is due to the changed ownership model and context of the potentially unsecure environments, in which an employee is using private or company owned devices and corporate data. To help reduce potential risks, we have suggested the adoption

of a 'soft' strategy of nudging that tries to influence the choices of employees by subtly pushing them towards more appropriate decisions, leaving the final choice and the responsibility for its consequences to employees. This approach can be used to optimize compliance with the company's Information Security policy. In addition, such an approach takes into account the ownership model and considers the dynamics of the context, in which employees might have more awareness of the situation to make an informed decision, than a policy maker can ever have.

When compared to more restrictive and less flexible Information Security policies, which leave no choice to decision makers, an alternative 'soft' nudging approach looks appealing when freedom of choice is at stake. This approach allows users to take responsibility, when dealing with corporate data/device, which may also be advantageous.

We considered several tested and potential examples of nudging in the security context and showed how users can be softly influenced towards choosing some of the options that are considered to be 'better' from security and or productivity points of view. At the same time nudging assumes that decision makers are well informed and are free to override nudges.

As future work, we are considering the development of rigorous risk assessment of trade-off solutions for concrete security scenarios to ground options towards which nudging is performed. It is a complex task of trading security and productivity objectives of a decision maker, while taking into account security policy of the company and the employee's personal preferences. We also aim to create a methodology to construct choice architectures in security, and to be able to evaluate the impact in corporate risk through nudging techniques.

## Acknowledgments

The authors acknowledge funding for "Choice Architecture for Information Security" (ChAISe) project EP/K006568/1 from Engineering and Physical Sciences Research Council (EPSRC), UK, and Government Communications Headquarters (GCHQ), UK, as a part of Cyber Research Institute. We would gratefully acknowledge the support and contribution of our colleagues on the ChAISe project from Northumbria University: Debora Jeske and Pam Briggs, who worked with us to identify issues and solutions in this project.

## References

[1] The Economist. (2011, October 8). *Consumerisation: The Power of Many*, Special Report: Personal Technology [Online]. Available: http://www.economist.com/node/21530921.

[2] SC Magazine. (2011, July 21). *New version of mobile security product launched by Trend Micro* [Online]. Available: http://www.scmagazineuk.com/new-version-of-mobile-security-product-launched-by-trend-micro/article/208014/.

[3] A.S. Hanks, D.R. Just and B. Wansink, "Trigger foods: The influence of irrelevant alternatives in school lunchrooms," *Agricultural and Resource Economics Review*, vol. 41, no. 1, pp.114-123, 2012.

[4] Behavioral Insight Team. (2012, February 24). *Applying behavioral insights to reduce fraud, error and debt*, Cabinet Office report, UK, [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60539/BIT_FraudErrorDebt_accessible.pdf.

[5] E.K. Chloe, J. Jung, B. Lee, and K. Fisher, "Nudging people away from privacy invasive mobile apps through visual framing," in *INTERACT 2013, Part III*, Lecture Notes in Computer Science, Springer, vol. 8119, no. 3, 2013, pp. 74-91.

[6] Y. Wang, P.G. Leon, K. Scott, X. Chen, A. Acquisti and L.F. Cranor, "Privacy nudges for social media: an exploratory Facebook study," in *Proceedings of the 22nd international conference on World Wide Web companion (WWW '13 Companion). International World Wide Web Conferences Steering Committee*, Republic and Canton of Geneva, Switzerland, 2013, pp. 763-770.

[7] A. Acquisti, "Nudging Privacy: The Behavioral Economics of Personal Information," *IEEE Security & Privacy*, vol. 7, no. 6, pp. 82-85, 2009.

[8] J. Turland, L. Coventry, D. Jeske, P. Briggs, C. Laing, I. Yevseyeva and A. van Moorsel, "Nudging towards security: Developing an application for wireless network selection for android phones," (in preparation)

[9] C. Morisset, T. Gross, A. van Moorsel and I. Yevseyeva, "Nudging for quantitative access control systems," in Human Aspects of Information Security, Privacy and Trust, T. Tryfonas, I. Askoxylakis (Eds.) Lecture Notes in Computer Science, Springer, vol. 8533, 2014, pp. 340-351.

[10] C. Morisset, I. Yevseyeva, T. Gross and A. van Moorsel, "A Formal Model for Soft Enforcement: Influencing the Decision-Maker," in *Security and Trust Management*, Lecture Notes in Computer Science, Springer, vol. 8743, pp. 113-128, 2014.

[11] D. Jeske, L. Coventry, P. Briggs and A. van Moorsel. (2014). "Nudging whom how: IT proficiency, impulse control and secure behaviour," in *CHI Workshop on Personalizing Behavior Change Technologies, CHI 2014* [Online]. Available: http://personalizedchange.weebly.com/1/post/2014/03/nudging-whom-how-it-proficiency-impulse-control-and-secure-behavior.html.

[12] I. Yevseyeva, C. Morisset, T. Gross and A. van Moorsel, "A Decision Making Model of Influencing Behavior in Information Security," in *Computer Performance Engineering*, Lecture Notes in Computer Science, Springer, vol. 8721, pp. 194-208, 2014.

[13] Tech Dep of ENISA. (2006, March 30). *Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)*, ENISA report 2006 [Online]. Available: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/information-packages-for-small-and-medium-sized-enterprises-smes

[14] BSI standards Publication, *BS ISO/IEC 27005:2011. British standard for Information technology – Security techniques – Information security risk management*, 2011.

[15] J. Clarcke, M.G. Hidalgo, A. Lioy, M. Petkovic, C. Vishik and J. Ward. (2012, September 28) *Consumerization of IT: Top risks and opportunities. Responding to the evolving threat environment*. ENISA report [Online]. Available: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/consumerization-of-it-top-risks-and-opportunities.

[16] J. Clarcke, M.G. Hidalgo, A. Lioy, M. Petkovic, C. Vishik, J. Ward and L. Marinos. (2012, December 19). *Consumerization of IT: Risk mitigation strategies. Responding to the evolving threat environment*. ENISA report. [Online]. Available: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COITMitigationStategiesPublishedVersion.pdf.

[17] H.H. Thompson. (2010, March 9). *Consumerization and security: Effective Security Practice Series.* Microsoft Corp. White paper. [Online]. Available: download.microsoft.com/download/E/F/9/EF9F24B7-DB49-44D4-8F6A-A49D5020B8B8/Consumerization_Final.pdf.

[18] MWR Infosecurity and CPNI. (2013, February). *Mobile Devices Guide for Implementers* [Online]. Available: http://www.cpni.gov.uk/Documents/Publications/Non-CPNI_pubs/2013-02-22-mobile_devices_guide_for_implementers.pdf.

[19] J. Hunt, "BYOD Policy – What Businesses Need to Consider," *Credit Control*, vol. 33, no. 5/6, p. 69, 2012.

[20] M. Savage. (2011, May 27). *IT consumerization drives new security thinking.* Information Security Magazine [Online]. Available: [SearchSecurity.com].

[21] A. Beautement, M.A. Sasse and M. Wonham, "The compliance budget: managing security behaviour in organizations," in *Proceedings of the 2008 workshop on new security paradigms (NSPW '08)*. ACM, New York, NY, USA, 2008; pp. 47-58.

[22] I. Kirlappos, S. Parkin and M.A. Sasse, "Learning from "Shadow Security: Why understanding non-compliance provides the basis for effective security," in *Proceedings of Workshop on Usable Security*, 2014.

[23] R.H. Thaler and C.R. Sunstein. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New Haven, CT, USA: Yale University Press, 2008.

[24] A. Fletcher, T. Marteau and T. Worsley. (2012, February 9). *Helpdesk report: Use of behavioral economics in development interventions*, Human Development Resource Centre [Online]. Available: http://www.heart-resources.org/wp-content/uploads/2012/05/Use-of-Behavioural-Economics-February-2012.pdf

[25] B.C. Kim and Y.W. Park, "Security versus convenience? An experimental study of user misperceptions of wireless Internet service quality," *Decision Support Systems*, vol. 53, no. 1, pp. 1-11, 2012.

[26] G.A. Miller, "The magical number seven, plus or minus two: Some limits on our capacity for processing information," *Psychological Review*, vol. 63, no. 2, pp. 81–97, 1956.

[27] P. Dolan, M. Hallsworth, D. Halpern, D. King and R. Metcalfe "Influencing Behaviour: The MINDSPACE way," *Journal of Economic Psychology*, vol. 33, pp. 264-277, 2012.

[28] L. Coventry, P. Briggs, D. Jeske, D and A. van Moorsel, "SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cybersecurity Environment," In *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience*. Lecture Notes in Computer Science, Springer, vol. 8517, 2014, pp. 229-239.

[29] G. Farnham and K. Leune. (2013, October 14). *Tools and standards for cyber threat intelligence projects* [Online]. Available: http://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375

[30] U.S. Air Force Software Protection Initiative. (2009, December 15). *The Three Tenets of Cyber Security* [Online]. Available: http://www.spi.dod.mil/tenets.htm

[31] ARS Technica. (2014, July). *"BadUSB" exploit makes devices turn "evil"* [Online]. Available: http://arstechnica.com/security/2014/07/this-thumbdrive-hacks-computers-badusb-exploit-makes-devices-turn-evil/

[32] Cyber Attacks Statistics. (2015, February). *Hackmageddon* [Online]. Available: http://hackmageddon.com/category/security/cyber-attacks-statistics/

[33] Black hat Conference. (2003). *Man in the middle attacks demo* [Online]. Available: https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-ornaghi-valleri.pdf

[34] Gawker. (2011). *The Facebook Setting You Should Change as Quickly as Possible* [Online]. Available: http://gawker.com/5744229/the-facebook-setting-you-should-change-as-quickly-as-possible

[35] Facebook. (2011). *A Continued Commitment to Security* [Online]. Available: https://www.facebook.com/notes/facebook/a-continued-commitment-to-security/486790652130

[36] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin and L. F. Cranor, "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms," In *Proceedings of the 2012 Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2012.

[37] M. Weir, S. Aggarwal, M. Collins and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010.

[38] R. Shay, S. Komandri, P. Kelley, P. Leon, M. Mazurek, L. Bauer, N. Christin and L. Cranor, "Encountering Stronger Password Requirements: User Attitudes and Behaviors," in *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2010.

[39] N. Malkin, S. Krishnamurthi and D.H. Laidlaw, "Poster: Waiting makes the Heart Grow Fonder and the Password Grow Stronger," In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2013.

[40] S. Fiorella. (2014, November 8). *The Insidiousness of Facebook Messenger's Android Mobile App Permissions (Updated)*. Huffington Post [Online] Available: Available online: http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-of-face_b_4365645.html

**Biographical notes**

**Iryna Yevseyeva**
Iryna Yevseyeva is a research associate at the Choice Architecture for Information Security (ChAISe) project at Newcastle University. She contributes to the project with her expertise in optimisation and decision making, in particular, in multi-criteria optimisation and decision analysis. Before joining Newcastle University in 2013, she was a post-doctoral researcher on multi-objective optimisation: in the Netherlands the Leiden Institute of Advanced Computer Science at the Leiden University in 2012-2013 on drug discovery; and in Portugal at the Polytechnic Institute of Leiria in 2011-2012 on spam filtering; at INESC Porto with Ciencia 2008 grant in 2009-2011 on scheduling; at the University of Algarve with grants from Academy of Finland and European Commission (Erasmus Mundus) in 2008-2009 on algorithms development. Iryna received PhD degree in computer science and optimisation from the University of Jyvaskyla, Finland, in 2007, for the research on multicriteria classification with applications in healthcare. Before joining PhD program in 2004, she worked as a software developer at the Niilo Maki Institute of Neuropsychology, Finland, in 2001-2003. She has Master of Science degree in mobile computing from the University of Jyvaskyla, Finland (2001) and Master degree with honours in information technology from the Kharkov National University of Radio-electronics, Ukraine (2000).

*www.shortbio.net/iryna.yevseyeva@newcastle.ac.uk*

**James Turland**
I am currently finishing my PhD in consumerisation and security modelling. I have worked on the Choice Architecture for Information Security (ChAISe) project for the past 18 months as a Research Associate at Newcastle University. I have a keen interest in security, specifically in understanding the role of the user and how technology can be adapted to build a more secure environment. Outside of my academic work I am an avid cyclist.

*www.shortbio.net/james.turland@newcastle.ac.uk*

**Charles Morisset**
Charles Morisset is a Senior Research Associate at Newcastle University, working with Aad van Moorsel on quantitative aspects of security, in particular in the decision making process and in access control mechanisms. Charles received is PhD from Université Pierre et Marie Curie - Paris VI in France in 2007, on the topic of formalisation of access control systems. He then worked from 2007 to 2009 at the United Nations University, in Macau SAR, China, on formal methods for software engineering, after which he joined the Information Security Group at Royal Holloway, University of London, to work on risk-based access control until 2011. From 2011 to 2013, he worked at the Istituto di Informatica e Telematica in Pisa, Italy, on formal methods and access control, and he joined the Centre for Cybercrime and Computer Security at Newcastle University in 2013.

*www.shortbio.net/charles.morisset@newcastle.ac.uk*

**Lynne Coventry**
Lynne Coventry is the Director of PaCT Lab (Psychology and Communication Technology) at the University of Northumbria. She is an applied researcher who enjoys working in multidisciplinary teams to solve real problems. She is keen to explore new ways of integrating psychology into design and technology development processes. While her early career was spent as a research fellow and lecturer at Stirling University, Heriot Watt and Dundee university, the majority of her career has been as a researcher within Industry (both computing and medical products) working to incorporate understanding of people, their use and acceptance of technology into the requirements and design process. Lynne is best known for her work on usable security, particularly authentication.

*www.shortbio.net/lynne.coventry@northumbria.ac.uk*

**Thomas Groß**
Thomas Groß is a tenured lecturer (assistant professor) in security, privacy and trust at the School of Computing Science at the University of Newcastle upon Tyne (since 2011). He is the director of the Centre for Cybercrime and Computer Security (CCCS), a UK Academic Centre of Excellence in Cyber Security Research (ACE-CSR). His research interests are in security and privacy as well as applied cryptography and formal methods. He was a tenured research scientist in the Security and Cryptography group of IBM Research - Zurich before that and IBM's Research Relationship Manager for privacy research. Thomas received his M.Sc. in Computer Science at the Saarland University, Germany, in 2004. He received his Ph.D. from the Ruhr-University Bochum, Germany, in 2009. His thesis was on the security analysis of standardized identity federation. Thomas is a member of the GI, ACM, IEEE, IACR and EATA, as well as Alumnus of the German National Academic Foundation.

*www.shortbio.net/thomas.gross@newcastle.ac.uk*

**Christopher Laing**
Dr Christopher Laing is a University Fellow in the Faculty of Engineering and Environment, and the Project Director of Northumbria University's Warning, Advice & Reporting Point. He is co-editor of 'Securing Critical Infrastructures and Industrial Control Systems', and a consultant for the European Network & Information Security Agency (ENISA). He has authored ENISA reports on Cyber-Bullying and Online Grooming and the Identification of Emerging and Future Risks, and he has worked with national law enforcement agencies in the development of postgraduate computer forensics/digital security programmes. He is currently Co-Investigator on EP/K006568/1: 'Choice Architecture for Information Security', part of the GCHQ/EPSRC Cyber Security Research Institute.

*www.shortbio.net/christopher.laing@northumbria.ac.uk*

**Aad van Moorsel**
Aad van Moorsel is a Professor in Distributed Systems and Head of School at the School of Computing Science in Newcastle University. His group conducts research in security, privacy and trust. Almost all of the group's research contains elements of quantification, be it through system measurement, predictive modelling or on-line adaptation. Aad worked in industry from 1996 until 2003, first as a researcher at Bell Labs/Lucent Technologies in Murray Hill and then as a research manager at Hewlett-Packard Labs in Palo Alto, both in the United States. He got his PhD in computer science from Universiteit Twente in The Netherlands (1993) and has a Masters in mathematics from Universiteit Leiden, also in The Netherlands. After finishing his PhD he was a postdoc at the University of Illinois at Urbana-Champaign, Illinois, USA, for two years. Aad became the Head of the School of Computing Science in 2012.

*www.shortbio.net/aad.vanmoorsel@newcastle.ac.uk*