Information Security and Privacy – Challenges and Outlook

Steven Furnell, Paul Haskell-Dowland, Manish Agrawal, Richard Baskerville, Anirban Basu, Matt Bishop, Jorge Cuellar, Sara Foresti, Lynn Futcher, Nurit Gal-Oz, et al.

Information Security and Privacy – Challenges and Outlook

Steven Furnell[1,2][0000-0003-0984-7542], Paul Haskell-Dowland[2][0000-0003-1365-0929], Manish Agrawal[3][0000-0001-7447-2367], Richard Baskerville[4] [0000-0003-2860-5215], Anirban Basu[5‡][0000-0001-5438-0959], Matt Bishop[6][0000-0002-7301-7060], Jorge Cuellar[7], Sara Foresti[8][0000-0002-1658-6734], Lynn Futcher[9][0000-0003-0406-8718], Nurit Gal-Oz[10][0000-0003-0565-8656], Teju Herath[11][0000-0002-3653-5643], Christian Damsgaard Jensen[12][0000-0002-0921-7148], Allen Johnston[13][0000-0003-0301-4187], Wouter Joosen[14], Giovanni Livraga[96][0000-0003-2661-8573], Javier Lopez[15][0000-0001-8066-9991], Stephen Marsh[16], Fabio Martinelli[17], Fabio Massacci[18][0000-0002-1091-8486], Aljosa Pasic[19], Stef Schinagl[20][0000-0002-4455-7287], Abbas Shahim[20], Kerry-Lynn Thomson[9][0000-0002-6456-9701], Jaideep Vaidya[21][0000-0002-7420-6947], Tony Vance[22][0000-0002-4554-6176] and Merrill Warkentin[23][0000-0001-7435-7676]

[1] School of Computer Science, University of Nottingham, UK
[2] School of Science, Edith Cowan University, Australia
[3] University of South Florida, USA
[4] Georgia State University, USA
[5] University of Sussex, UK
[6] University of California at Davis: Davis, California, USA
[7] University of Passau, Germany
[8] Università degli Studi di Milano, Italy
[9] Nelson Mandela University, South Africa
[10] Sapir Academic College, Israel
[11] Brock University, Canada
[12] Technical University of Denmark (DTU), Denmark
[13] University of Alabama, USA
[14] KU Leuven, Belgium
[15] University of Malaga, Spain
[16] University of Ontario Institute of Technology, Canada
[17] CNR, Italy
[18] University of Trento, Italy
[19] ATOS, Spain
[20] VU Amsterdam, Netherlands
[21] Rutgers University, USA
[22] Temple University, USA
[23] Mississippi State University, USA
steven.furnell@nottingham.ac.uk

Abstract. The ongoing demand for new and faster technologies continues to leave consumers and business users to face the constant challenge of updating systems and software. This unrelenting pace of technological evolution has not always been matched with a commensurate focus on security and privacy matters. In particular, the obligatory move to embrace cloud and IoT - that frequently result in the collection and analysis of large data lakes has raised challenges for

sovereign data protection and privacy legislation where data at rest can change overnight with mergers and acquisitions of service providers. This chapter examines the role of IFIP Technical Committee 11 (and its 14 underlying Working Groups) in this ever-changing and evolving domain. The discussion provides an outline of key issues in information security when viewed from technical, organisational and human perspectives, which collectively represent the breadth of areas within which TC-11 and its Working Groups are seeking to make contributions. The chapter as a whole gives a clear sense of the challenges involved in achieving and maintaining security and privacy, alongside insights into the ways that they are being tackled within IFIP activities.

Keywords: Information Security, Privacy.

1 Introduction

Alongside the global adoption and significant growth of information and communication technologies, comes the need to provide protection against potential breaches of security. These may result from deliberate and targeted attacks, as well as from misuse, inadvertent user errors, and system failures. In addition, with the volume and sensitivity of the related data that these systems store and communicate, there is an essential need to consider provisions for ensuring and maintaining privacy [1].

In recognition of these issues, IFIP Technical Committee 11 (TC-11) exists to increase the trustworthiness and general confidence in information processing, as well as to act as a forum for security and privacy protection experts and others professionally active in the field [2]. In parallel with the increasing importance of cyber security issues and concerns, the scope and activity of TC-11 has grown over the years, and at the time of writing encompasses 14 Working Groups, each focusing upon defined areas within the security and privacy landscape [3]. For the purpose of this chapter, each of the groups was asked to outline the challenges that they perceive in the future, resulting in the identification of a range of topical issues that can be broadly classified under the themes of technological, business and organisational, and human challenges. While each of these themes is distinct, this chapter considers how each of these perspectives combine and reflect the function of the Technical Committee while maintaining independent activities within each group. As may be expected, each working group approaches the issues of information security and privacy through the lens of their group role and scope.

After a short introduction to the working groups, this chapter first looks at the technological issues facing the ICT domain with consideration of the significant changes seen in recent years with new technologies and working approaches. The functional issues within organisations are then considered with due regard to policy, procedure and governance as well as a recognition of the changing (often global) legal frameworks in which ICT professionals must now function. Finally, the critical issue of human factors is considered. This is often overlooked but is a vital factor in ICT systems as humans design, implement and use the very systems that are then the cause of many security and privacy concerns.

2 Overview of Technical Committee 11

Technical Committee 11 (formally titled Security and Privacy Protection in Information Processing Systems) was originally established in 1983, and has the overall remit to:

- establish a common frame of reference for security and privacy protection in organizations, professions and the public domain;
- facilitate the exchange of practical experience;
- disseminate information on, and the evaluation of, current and future protective techniques;
- promote security and privacy protection as essential elements of information processing systems;
- clarify the relation between security and privacy protection.

Since its inception, TC-11 has grown to be supported by 14 Working Groups [3] covering a diverse range of security-oriented areas.

11.1 Information Security Management

There is a growing trend for senior business management to be held answerable for the reliable and secure operation of their information systems, as they are for control of their financial aspects. Information Security is, and should always be, an obligation on upper management with appropriate delegated responsibility [4]. Information security professionals and WG 11.1 in particular, should therefore be responsible for the development of all types of tools, mechanisms and methods to support top management in this new responsibility.

11.2 Pervasive Systems Security

Pervasive systems shall be defined to be large scale systems that are comprised of nodes ranging from RFID tags, through embedded systems, to personal mobile devices, interconnected by a mixture of short-range wireless and wide are wired networks. The typical characteristics of a pervasive system are: resource constrained nodes, often physically unreachable or without user interface, whose interconnections often span a large number of administrative domains with conflicting interests. Security of such systems is therefore an emergent property.

11.3 Data and Applications Security and Privacy

IFIP WG 11.3 was formed in 1986 to stimulate activities in both data security and privacy research and in the application of data security and privacy techniques. The goal in forming the working group was to encourage the development of better techniques for stating data security and privacy requirements, for designing, building, and implementing data management systems that satisfy security and privacy requirements, and for assuring that the systems meet their requirements in actual operation.

11.4 Network & Distributed Systems Security

Management in any organization is responsible for the reliable and secure operation of the information systems that support the organization. As inter and intra-organization networking between information systems become the rule as well as the daily operational environment, the scope of concern takes on new aspects and new technical details come into play. Management must not only address the security issues of wholly internal systems together with any networks to which they might be connected, but also must assure that the protective mechanisms installed in them are not accidentally or intentionally thwarted or subverted by other systems with which data exchange connections are established.

11.5 IT Assurance and Audit

The current attention for digitalization and regulatory compliance has significantly changed the way in which IT has been organized, managed and consumed. Given their strict corresponding control objectives, organizations must transparently prove that they act in accordance with the applicable laws and regulations and manage digital risk in a proper fashion. Hence, reasonable assurance with respect to IT is crucial in this case to build confidence whether IT solutions and underlying infrastructures preserve resources, maintain data integrity as well as availability, meet the service levels, satisfy the regulatory requirements and accordingly assist in attaining their goals. For this essential purpose, a number of IT assurance and audit engagements are normally conducted. The aim of the working group is to study and develop detailed knowledge on IT assurance and audit models, standards, processes and techniques to meet the needs of organizations from a wider business perspective.

11.6 Identity Management

The aim of WG11.6 is to promote - through education, research and outreach - the awareness and understanding of issues including identity management applications and methodologies, identity management issues at the national level (including issues of federated and multilateral identity management), and the role and effectiveness of identity management in fighting fraud and other forms of crime [5]. The working group is also specifically interested in biometric technologies that increasingly contribute to the IM landscape, including legal and operational aspects of biometrics, methods and techniques that can help to evaluate and improve the technologies, and their associated impact upon society [6,7].

11.7 Information Technology: Misuse and The Law

The WG focuses on the relations between IT Misuse, the Law and Society. As “Misuse” depends very much on the point of view and the cultural background of the viewer a very broad understanding of the term “Misuse” turned out to be appropriate. The WG studies technical, organisational, legal and social aspects of information infrastructures and electronic services with regard to their trustworthiness. The emphasis is on legal implications of new technology and vice versa.

11.8 Information Security Education

The aim of WG11.8 is to promote information security education and training in university, government and industry through the encouragement of the development of course models [8]. The WG also aims to establish an international resource center for the exchange of information about education and training in information security and to collect, exchange and disseminate information, relating to information security courses conducted by private organizations for industry [9]. The WG further aims to collect and periodically disseminate an annotated bibliography of information security books, feature articles, reports, and other educational media.

11.9 Digital Forensics

The growth of the Internet and the plethora of technology devices has resulted in more and more information being stored, transmitted and processed in digital form than ever before [10]. At the same time this connectivity is also enabling criminals to act transjurisdictionally with ease. Increasingly we are witnessing that a perpetrator of a crime is being brought to justice in one jurisdiction while the digital evidence needed to prosecute the perpetrator residing in other jurisdictions. This requires that all nations have the ability to collect, preserve and examine digital evidence for their own needs as well as for the potential needs of other nations. Digital Forensics is the scientific study of the processes involved in the recovery, preservation and examination of digital evidence, including audio, imaging and communication devices with consideration of forensic evasion techniques [11]. The efforts of the working group in digital forensics strive to discover, define and foster fundamental scientific principles that support the investigation of digital wrongdoings from all perspectives, legal, business and military.

11.10 Critical Infrastructure Protection

The "information infrastructure" – comprising computers, embedded devices, networks and software systems – is vital to day-to-day operations in every sector: agriculture, food, water, public health, emergency services, government, defense, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping [12]. Global business and industry, governments, indeed society itself, cannot function effectively if major components of the critical information infrastructure are degraded, disabled or destroyed [13]. Working Group 11.10 on Critical Infrastructure Protection seeks to engage the international information security research community to work together on applying scientific principles and engineering techniques to address current and future problems in information infrastructure protection. In addition to engaging the research community, the WG draws other interested parties (government agencies, infrastructure owners, operators and vendors, and policy makers) in a constructive dialog on critical infrastructure protection.

11.11 Trust Management

The deployment of a global computing infrastructure raises new and difficult security and privacy issues. Global computing allows entities to reason about the trustworthiness

of other entities and to make autonomous security decisions on the basis of trust. This requires the development of a computational trust model that enables entities to reason about trust and to verify the security properties of a particular interaction [14]. The global computing infrastructure is highly dynamic with continuously appearing and disappearing entities and services [15]. It is vital that the associated computational trust model is able to incorporate this dynamism and that equally flexible legislative and regulatory frameworks emerge.

11.12 Human Aspects of Information Security and Assurance

Achieving security within information systems is no longer simply a technical problem but increasingly involves the active participation of people in order to securely design, deploy, configure and maintain systems [16]. Whilst the level and sophistication of this interaction may vary; anyone who is engaged with technology, from administrators of the most complex of IT systems to owners of simple devices, all need to make decisions that have an impact on the security and privacy of their device and information. Unfortunately, while people represent a key facet in achieving security, evidence demonstrates that this is often the point of failure [17]. With security now impacting all aspects of society, from the young to old, enterprise organisation to the individual, it is imperative that systems are designed, policies are put in place that assist people in ensuring the security of their systems. It is against this context that Working Group 11.12 aims to contribute.

11.13 Information Systems Security Research

The aim of the working group is the creation, dissemination, and preservation of well-formed research about information systems security. While relevant for advanced practical development, our primary audience consists of researchers in this area. We value research products with highly reliable and validated theory, empirical data, or quantitative/qualitative social scientific methodology.

11.14 Secure Engineering

The Information and Communication Technology (ICT) landscape is continuously changing. We are now witnessing the emergence and consolidation of unprecedented models for service-oriented computing (SOC): Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [15,18]. These models have the potential to better adhere to an economy of scale and have already shown their commercial value fostered by key players in the field. Nevertheless, those new models present change of control on the applications that will run on an infrastructure not under the direct control of the business service provider. For business-critical applications this could be difficult to be accepted, when not appropriately managed and secured. These issues are of an urgent practical relevance, not only for academia, but also for industry and governmental organizations [19]. New Internet services will have to be provided in the near future, and security breaches in these services may lead to large financial loss and damaged reputation.

There thus the need and opportunity to organize, integrate and optimize the research on engineering secure services and related software systems to deal effectively with this increased challenge is pertinent and well recognized by the research community and by the industrial one.

3 Technological issues

The ICT landscape is continuously changing. For example, we have seen the consolidation of models for service-oriented computing (Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)), the increased use of automation, and the emergence of new paradigms such as cloud and the Internet of Things (IoT). However, new developments open up the potential for vulnerability to new threats (or indeed old threats in new guises). As such, some of the consequent challenges are perceived to be:

- maintaining effective cyber defence, as technology and functionality grow faster than security;
- achieving trust in devices specially when they operate remotely;
- security and interoperability of new communication technologies;
- the fact that evidence has moved from being on media in a computer in a single location to existing in myriad locations and forms (e.g. mobile devices, distributed internet-enabled (IoT) electronics, and on corporate controlled servers with server-side processing and storage).

These challenges create fundamental requirements in relation to security engineering, but they also create knock-on implications for issues such as incident handling, response, and forensic investigation, where the scale and complexity of systems calls for new capabilities to maintain effectiveness. Security professionals are also having to address the growing threat to critical infrastructure where industrial control systems (ICS) are connected to operational networks and even to the public Internet [20]. With technology continuing to evolve, the distributed nature of infrastructure will increase and the expansion of autonomous vehicles and increased artificial intelligence/machine learning will all present significant challenges to the security community.

3.1 Securing applications and data

Data are today the new oil, as the ability to collect, share, process and analyse data are at the centre of the great advancements we are enjoying in our society. Providing effective techniques for ensuring proper security and privacy is of utmost importance, for both enabling such advancements (as fear of exposure of private information can have detrimental impact on their adoption) as well as enabling their development (as by developing techniques for ensuring data protection can widen the range of scenarios where data can be used).

The evolution of ICT has radically changed our lives, enabling information to be available from anywhere at any time. The growing availability of computational power

and network connections at competitive prices facilitates collecting, sharing, processing, and accessing huge amounts of information. Thanks to the wide diffusion of devices collecting information (e.g., IoT devices, smart meters, fitness bands) and of personal devices connected to the network (e.g., smartphones, tablets, laptops), the amount of data generated on a daily basis by companies and final users has grown exponentially and is expected to grow at a continuously increasing rate in the future. Also, the cost of data storage and processing has significantly decreased, enabling the long-term storage and analysis of data and making it accessible when needed. Pictures and videos can be stored in the cloud, analysis performed over huge data collections, third party computational power purchased or leased for heavy elaborations, information collected from sensors spread in the environment where we live, appliances controlled in our houses from a smartphone. These are only a few examples of the advantages of living in a globally interconnected society, where every object is a smart object and anything we need is available from anywhere and at any time.

The advantages of the technological evolution, however, do not come for free as they introduce unprecedented security and privacy risks, due to the increased amount of (possibly sensitive) information collected, stored, and distributed, and to the loss of control of data by their owners when external subjects are involved in the information lifecycle. Users are becoming more and more concerned about their privacy, since collected data can be used to identify individuals and/or infer information that was not intended for disclosure – permission often being provided unknowingly through terse terms and conditions [21]. The location information collected by our phones, the pattern of walking recorded by surveillance cameras, seemingly innocuous information provided when subscribing to a service (e.g., date of birth and city of residence), biometric information used for authentication, are only a few examples of data that can be exploited to identify the person to whom they refer. Sensitive information not intended for disclosure is often collected by devices such as: fitness bands, home assistants, smart home appliances and sensors, social networks, just to mention a few. In all these scenarios, users are not in control over their own data and their privacy is possibly at risk. Indeed, users are often not even aware of the fact that data about themselves are collected and/or cannot control the collection, storage, use, analysis, or deletion of their data [22]. The loss of control is one of the problems slowing the wide adoption of externalized services (cloud, fog, and edge scenarios as well as digital data markets) as an enabling technology for data storage and elaboration. While external providers can be considered reliable for guaranteeing basic security protection (e.g., protection from unauthorized accesses to data and resources by external third parties), they might not be considered trusted for confidentiality (i.e., authorized to know the data content) or for guaranteeing integrity of the data they store or process. Many challenges need to be addressed to guarantee proper security and privacy in the emerging scenarios, including the need to provide confidentiality and integrity of data stored at, shared with, or processed by external parties, while providing needed access and computational functionalities [23]. Advancements in artificial intelligence, which on one side may make the data more exposed and hence user privacy more at risks, can also help in developing better techniques for ensuring protection of information.

The problem of data security and privacy is evolving with technology: the technological evolution provides benefits, but also introduces new vulnerabilities. Data security and privacy in the modern digital society are complex concepts that require attention from several points of views (e.g., legal, social, economic, technological) and raise novel challenges that need to be addressed to enable users to fully enjoy the advantages of technological evolution [17].

3.2 Engineering for better security

While the service-Oriented Computing (SOC) models bring significant savings and convenience for organisations and users alike, they also introduce challenges for the security engineering community. These models have the potential to better adhere to an economy of scale and have already shown their commercial value fostered by key players in the field. Nevertheless, those new models present change of control of the applications that will run on an infrastructure not under the direct control of the business service provider. For business-critical applications this could be difficult to be accepted, when not appropriately managed and secured. These issues are of an urgent practical relevance, not only for academia, but also for industry and governmental organizations. New Internet services will have to be provided in the near future, and security breaches in these services may lead to large financial loss and damaged reputation.

There is a need to organize, integrate and optimize research on engineering secure services and related software systems. This challenge is well recognized by the research and industrial communities.

Some of the specific challenges that need to be addressed in security engineering include:

- Security requirements engineering
- Secure Service Architectures and Design
- Security support in programming environments
- Service composition and adaptation
- Runtime verification and enforcement
- Risk and Cost-aware Secure Service Development
- Security assurance and certification
- Quantitative security for assurance

3.3 Investigating the inevitable

Historically, the focus of digital forensics, incident response and electronic discovery has been on gathering evidentiary trace from desktop computers and small enterprises. While the processes and formalisms remain the same, where the evidence is found, and the volume of evidentiary sources has led to some fundamental challenges. Currently, evidence has moved from being on media in a computer in a single location to existing in mobile devices, internet enabled (IoT) electronics, and on corporate controlled servers with server-side web processing and storage. Additionally, enterprise computing has increased and evolved with data being stored in a myriad of forms in appliances,

services, and alternative compute architectures. The digital forensics community needs verifiable and validated capabilities to address these changing computing environments. This is further complicated by the use of service-oriented computing with storage and processing of data moving from on-premise to frequently cloud-based locations. This also introduces complex legal problems with the potential for multi-jurisdictional investigations.

4 Business and organisational issues

The current attention for regulatory compliance has visibly changed the way in which IT has been organised and managed. Given their strict corresponding control objectives, organisations must transparently prove that they act in accordance with the applicable laws and regulations. This gives rise to a number of challenges, that collectively span areas such as information security management, audit and governance:

- ensuring adherence to organisational information security policies and procedures;
- transparently proving that organisations are acting in accordance with the applicable laws and regulations;
- better techniques for stating data security and privacy requirements, for designing, building, and implementing data management systems that satisfy security and privacy requirements, and for assuring that the systems meet their requirements in actual operation;

Reasonable assurance with respect to IT is crucial in this case to build confidence whether IT solutions and underlying infrastructures preserve resources, maintain data integrity as well as availability, meet the service levels, satisfy the regulatory requirements and accordingly assist in attaining their goals.

4.1 The role of audit and IT assurance

Today's audit implications are associated with the view on digitalization and the impact of this technology-centric and global phenomenon on the business strategies across the globe. The centre of this digital journey is dominantly filled in by the far-reaching deployment of technology. The intensive use of this evolutionary capability empowers to reinvent business models, improve customer experience, optimize processes and operations, reshape the trade with partners, and more. It is all needed to remain attractive in the modern digital chains, and survive in the current ever-demanding marketplace. It has become a technology-driven environment and business climate that seems not to tolerate low-techs, and appears not to accept the large distances between the traditional physical world and the new digital world any longer. We are entering an age in which the technology defines the bright future, and dictates the way in which we conduct business and how we live our lives.

IT has already become business. This continuously evolving technology forms the beating heart of organizations, and is thus almost a core part of a day-to-day responsibility of average business officials as well as top executives. Their changing view and

act for strategizing, steering, transforming, positioning, governing, managing, and running organizations in the digital age calls for a revamped orientation of IT auditing to remain as relevant as before.

A key finding of research among business leaders and Chief Executive Officers (CEOs) with respect to the key business issues facing their organizations was about the new and higher level of risks created by the digital era which are not properly dealt with [24,25]. This demanding world characterized by a technology-centric perspective requires a broader and more balanced picture of IT auditing that shifts the focus from controlling "around IT" towards the hard-core side of IT, and with the use of IT. The purpose is to concretely discover the technical details about the reality of IT, just the way it is without vagueness. In this challenging context, IT auditing is perceived as an instrument that can provide an independent and objective opinion on the extent to which IT is adequately controlled to ensure that this technology does not affect the risk profile of business practices. In addition, this global discipline can help to address risks and governance concerns so that insight is obtained into the gained degree of trust and acceptance as well as the achieved level of strategic progress and performance.

The demand for IT auditing and control has never been greater. But then, this growing need also implies that a new day has come that imposes to frequently, if not constantly, audit and control through IT and with IT because of the highly ever-increasing level of reliance on technology. However, research in this area is scarce and requires attention to initiate a wide range of studies in this field.

4.2 Establishing Trust in an untrusted environment

ICT systems, often known as Supervisory Control and Data Acquisition (SCADA) systems, control our critical infrastructure and are increasingly used to control production of products (known as "Industry 4.0") and services, e.g. through e-Government, Big Data and Cloud Services. IoT and digital communication technologies are forming the fabric of our social interactions through Social Media (SoMe) that have also become the primary source of information and news for many people. In order for humans to live and thrive in this environment, it is essential that they are able to trust the ICT infrastructure on which their existence depends.

Trust management technologies address the problems of how people can build trust in each other across computer networks (inter-personal trust), how people can decide what devices and infrastructure to trust (personal-device trust and infrastructure trust), and how components in computer systems and networks can reason about the trustworthiness of other system components (inter-device trust).

Inter-personal trust is generally based on a combination of personal experience, recommendations from a trusted entity or the reputation of the other party. Personal experience requires the ability to authenticate, or at least recognize, other entities, observe, and record the behaviour of these entities. This implies a study of entity authentication and entity recognition mechanisms, message authentication and authenticated encryption primitives, and mechanisms supported by secure hardware modules, e.g. remote attestation technologies, but also secure and authenticated storage technologies, such as digital signatures and blockchains. Recommendations are authenticated statements

regarding one named entity made by another and trusted entity. As such, the technological challenges are very similar to the challenges that arise in building personal experience, e.g. recommendations are commonly carried in digitally signed certificates. The value of recommendations depend on the ability to authenticate the named entity. Reputation systems aggregate behavioural information about a named entity from a multitude of sources. Depending on the reputation system, the behavioural information may be verified and the named entity as well as (some of) the behavioural information providers may be authenticated by the system; the identity of the source of reputation information is not always made available to the users of the reputation system. The success of a reputation system depends on the ability to ignore malicious or incompetent input and the aggregation mechanism, which is typically based on simple heuristics, statistical analysis, machine learning, game theory or other theoretical frameworks.

The aims of trust management, in a business and organisational context, is to support a virtuous circle of formation, distribution, exploitation and evolution of trust in other entities in the system. This means that the many challenges are similar to the challenges outlined above and that trust management technologies may help people decide which businesses or services to rely upon or what information to believe

Human society is built on trust and people need assurance that the environments, technologies and social relationships that they rely on continue to function in the ways they expect. In particular, the technology (devices and services) that they employ must work to their benefit at a visible and reasonable cost. One societal problem that trust management technologies may help to address is “fake news” (or other forms of fake information).

Trust management is by nature a “horizontal” multi-disciplinary area that brings together communities to support “vertical” areas such as reputation systems, security, identity and access management, social networks, risk and compliance, formal models, legal IT, economics, etc.

5 Human issues

The human aspect has traditionally, but often unfairly, been portrayed as the weakest link in cybersecurity. Unfortunately, adversaries are indeed likely to target people where they are perceived to be the route to exploitation, and it is also important to ensure that people themselves do not act in ways that introduce avoidable vulnerability. Key areas for attention are considered to include the following:

- the growing volume of threats that explicitly target the human element, such as increasingly sophisticated social engineering and phishing scams;
- major cybersecurity skills gap that needs to be addressed through formalised education;
- addressing resistant user attitude and resistant behaviour to information security by fostering an information security/cybersecurity culture.

Without effective consideration of the human aspect, the overall protection of systems and data will remain sub-optimal. We need to find effective means to support

people and help them engage, while at the same time protecting them from the attacks that seek to directly exploit them.

5.1 Addressing the human factor

The problem with the focus on human weaknesses is that humans are solely viewed as 'threats' and 'risks' to the organisation. However, it can be argued, that this is only one dimension of the human aspects of cybersecurity and that humans could become the best defence an organisation has to actively defend against cyberattacks. In order to empower employees to become part of the cybersecurity defence of an organisation, there must be a conscious effort to foster an information or cybersecurity culture in an organization [26]. Both sides of the human aspects of cybersecurity, the threats and the defence, should be acknowledged and addressed. Having said that, there are many challenges related to the human aspects of cybersecurity which are discussed below.

Many organisations implement complex technological controls to protect their network perimeter from external threats, as the perception often is that the greatest threats come from attackers outside the organisation. However, insider threats can be particularly dangerous for organisations, as insiders have legitimate access to information systems to accomplish daily tasks. There are typically two broad types of insider threats; malicious users (employees who willfully extract data) and negligent/apathetic users (employees who are careless about cybersecurity).

Malicious users are those who purposefully try to benefit themselves at the organisation's expense or directly damage the organisation. They might steal confidential data, commit financial fraud or sabotage IT systems because they are disgruntled. Malicious insiders are notoriously difficult to identify. However, technological controls, such as behaviour analytics, anomaly detection, threat intelligence and predictive alerts, can be used to attempt to identify and mitigate against malicious users and their actions. Fortunately, for most organisations, malicious users are the exception and not the rule.

However, one of the greatest challenges organisations may face is human error introduced through negligent or apathetic users. Negligent or apathetic users are those who are not aware of or do not realise how important cybersecurity is for an organisation. These users do not appreciate the important role they should play in protecting an organisation from cyberthreats. One of the major challenges with regard to these users is social engineering. Social engineering is the psychological manipulation of users to exploit them into performing actions for, or divulging information to, the attacker. There are a wide variety of social engineering attacks, including, but not limited to; phishing, pretexting, baiting and quid pro quo. Social engineering attacks rely on building trust relationships with targets, and then exploiting these relationships for gain (usually financial).

From a societal point of view, there are a number of cyber vulnerabilities related to both adults and children. Cyberbullying is an online form of traditional bullying where cyberbullies send threatening or humiliating messages to their adolescent victims, and can lead to depression, isolation, illness and, sometimes, suicide.

In addition, social media platforms continue to be very popular ways for people to keep in contact with friends, upload content and share information online. However,

there are many privacy concerns related to these social media platforms, for example, many users being unaware of the extent to which their personal information is spread after sharing.

Another societal challenge that is seemingly on the rise is that of fake news. One of the difficulties is that different people have different views of fake news. For many, fake news is seen as it was intended – false information being spread. For others, fake news is seen as anything that goes against their own beliefs or biases. The issue is that, more than making people believe false information, the rise of fake news is making it harder for people to see the truth. In other words, people may become less informed.

Most of these challenges can start being addressed by raising the awareness of both employees and society in general to cyberthreats. The cybersecurity awareness, however, must go further through cybersecurity educational programs to provide a deeper understanding of why cybersecurity is important and the role they should be playing in the defence of their organisation. Often, however, these programs are generic and are not very effective in addressing users and the threats they may be introducing, which may result in people developing the 'it won't happen to me' mindset. Therefore, information and cybersecurity awareness and education programs should be specifically contextualised to become relevant to the audience to ensure they become advocates for information and cybersecurity.

In organisations, for example, as part of management's duties, an organisational vision for cybersecurity should be expressed in policies. These policies should be enforced to assist management in curbing incorrect behaviour in their organisation and, ultimately, change the corporate culture. Transforming the corporate culture, however, takes time and perseverance, as it entails the unlearning of beliefs and changing the attitudes of employees, which can be a painful process [27]. The fostering of an information or cybersecurity culture in an organisation could, ultimately, positively influence the attitude and behaviour of employees towards information and cybersecurity. Although an organisation can never completely eliminate the cybersecurity risk posed by humans, the chances of a breach could be reduced if the cybersecurity education of users is made a priority.

Raising awareness and providing access to educational programs for the general public could also assist in creating a societal cybersecurity culture.

5.2 The importance of education

Many organizations, nations, businesses, and individuals are actively seeking to expand their knowledge of, and skills in, cybersecurity. Unfortunately, the amount of misinformation in this area, and the shortage of skilled, knowledgeable cybersecurity practitioners and experts, inhibits the ability to protect information and cyberinfrastructure. Worse, some organizations and individuals do not understand the need to protect themselves, or believe their measures are adequate when in reality they are not. The only cure for this lack of personnel, knowledge and understanding of how to determine and implement measures necessary for protection, is education.

This skills gap requires a multi-faceted solution with a combination of not only formalised education, but also training and awareness programs. It is also important to

recognise that for most government departments, organisations and businesses, security is rarely achieved without some impact on performance, usability or cost.

Current estimates indicate that there are about 1 million unfilled cybersecurity positions worldwide, potentially rising to 3.5 million by 2021 [28]. In order to address this rapidly increasing demand for cybersecurity skills, academic institutions worldwide are introducing and adapting courses and programs to teach students about information and cybersecurity. Among the main concerns for academics in computing, however, is what cybersecurity and related topics to cover and to what depth, as most computing courses already cover an expanse of content.

This broad domain encompasses an extensive set of technologies and concepts that can be taught in various ways. Current research in this domain covers both technical aspects (secure programming, network security, offensive security, cryptography, etc.) and human aspects (privacy, social engineering, cyber law, ethics, etc.). In addition, one of the key challenges is to ensure that the methods for teaching and learning in this domain are adapted to suit the specific context. This field is somewhat unique in terms of its cross-cutting multi-disciplinary nature. A further challenge is therefore to inculcate the principles of information and cybersecurity into even the most basic and entry-level courses.

A panel discussion during WISE11 highlighted some of the main challenges of building national cybersecurity workforces. These included how to estimate the size and make-up of national cybersecurity workforces based on needs; how to characterise such workforces; and how to achieve balance between employing organisation's priorities and national needs. During this panel discussion it was also noted that these challenges and the role of educational institutions in addressing the cybersecurity skills gap may differ across nations.

In 2017, a joint task force developed guidelines for undergraduate cybersecurity education programs. The resulting document, the Cybersecurity Curricula 2017 [29], addressed academic aspects of some of these challenges regarding the cybersecurity workforce and skills demand.

Further challenges will include the use of online technologies (for example, MOOCs) to share information and cybersecurity teaching and learning content and how training programs and academic education programs can work together to provide both practical experience and a deeper understanding of why the practical material works. This way, practitioners can adapt their knowledge and experience to circumstances beyond that covered in the training and in their environment, and academics can better understand the problems encountered in practice, and learn how to prevent those problems or handle them.

As noted above, the need for cybersecurity is generally understood. But its practice must be balanced with the cost in financial and human terms, and all too often the latter dominates the need. The need to strike an appropriate balance, and how to do so, will dominate much of the field in the near future.

5.3 The value of research

The challenges of behavioral compliance are focused on the adoption and use of protective security practices by individuals seeking to benefit themselves or their firms, or to avoid any negative consequences that may occur from non-adoption or misuse of security procedures and methods. Substantial research efforts have focussed on policy related compliance, but other forms of compliance, such as digital warnings, communicated alerts, and compliance with emerging technical standards have also appeared more recently. It is likely that this area of focus will continue to be of great interest for the foreseeable future.

Another primary challenge of interest is the problem of risk management. As described in the MIS Quarterly curation [30], the problem of risk management by security scholars has been mostly approached from a normative lens. Research over the years has addressed risk management through a variety of frameworks, models, and management techniques, with focused efforts made toward the extension and contextualization of managerial frameworks and theories that help to measure and control risk at the individual level.

Moving forward, emerging challenges such as neurosecurity (neurophysiological data collection), forensics analysis, and the behavioral analysis of design science treatments that enhance or balance security and privacy trade-offs will be explored. There is a new scale and scope of organizational and managerial challenges that are created by the growing prevalence of advanced persistent threats, securing blockchain data structures, protecting privacy in big data analytics, and the looming potential of commercial cyberspace collisions between defensive AI and offensive AI, and the cryptanalysis capabilities of quantum computing.

6 Future opportunities

Many of the areas discussed in the chapter serve to highlight opportunities for future research, and the Working Group agendas will be shaped accordingly. Space does not permit all of them to be catalogued and explored in this chapter, the magnitude of the challenge can be illustrated by homing in on a single area and looking at the issues that the related Working Group has identified as requiring attention. To this end, we present an example of some issues from WG11.5 in relation to IT auditing.

Organizations are turning into open and global digital factories that are built around customer experience, speed, agility, mobility, cost, automation, connectivity, and accuracy to drive success. Given this present and future reality, IT auditing can no longer be a profession that suffices with a tick-in-the-box examination without a clear orientation. To provide digital value and capture it we provide a House of IT Auditing, Fig. 1. The House of IT Auditing includes three main components of IT audit research that we consider the main areas of interest. The first area is concerned with the foundation of the profession: technology (e.g. cloud and digital platforms). It is put right at the center of business models, thereby becoming the beating heart and the base of modern organizations. The second component is related to the strategic pillars linked to the foundational developments: cybersecurity, analytics, and regulatory. Being exposed to

serious dangers, data-minded, and subject to laws and regulations are simply accepted as facts of today's life. The third and last component pertains to the professional support that can be provided to make a desired and recognized contribution. It is about the delivery of support in the areas of most need: assurance, advisory, and financial audit.

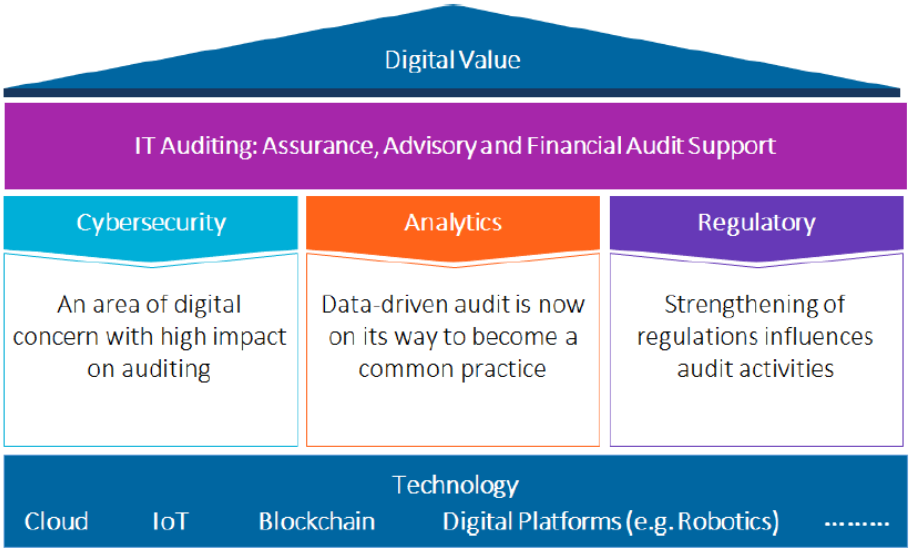

Fig. 1. House of IT Auditing.

7 Conclusions

The collective challenges across these areas are considered to be of increasing importance, especially in the context of emerging technologies (e.g. Cloud, IoT) that collect and analyse large data collections, and serve to further amplify the potential for impact in the event of security incidents and breaches. At the same time, there are also potential solutions that can work across the areas, such as the potential for AI technology to defend the human user from malicious hackers, rather than the human trying to recognize malicious intent. This in turn has the potential to serve and support the business objective in terms of effective governance and compliance.

8 Acknowledgments

We would like to acknowledge the contributions from working group officers and members in addition to the named authors of this chapter. Specifically: Raja Naeem Akram, Kam-Pui Chow, Richard George, Konstantinos Markantonakis, Gilbert Peterson, Damien Sauveron and Sujeet Shenoi.

‡Anirban Basu works at Hitachi R&D within Hitachi Ltd. The views, opinions, and/or findings contained in this article are those of the authors. These are not related to work at Hitachi and should not be interpreted as an official Hitachi position, policy, or decision, unless so designated by other documentation.

References

1. OECD, 2013, The OECD Privacy Framework, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, last accessed 16/12/2020
2. IFIP TC11, n.d., Aims and Scope, https://www.ifiptc11.org/aims-and-scope, last accessed 16/12/2020
3. IFIP TC11, n.d., Working Groups, https://www.ifiptc11.org/working-groups, last accessed 16/12/2020
4. Connolly L., Lang M. and Tygar J.D., Managing Employee Security Behaviour in Organisations: The Role of Cultural Factors and Individual Values, ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014, pp417-430
5. Wiefling S., Iacono L.L. and Dürmuth M., Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild, ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, pp134-148
6. Giorgi G., Martinelli, F., Saracino A. and Sheikhalishahi M., Walking Through the Deep: Gait Analysis for User Authentication Through Deep Learning, ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC2018, Poznan, Poland, September 18-20, 2018, pp62-76
7. Diaz-Tellez Y., Bodanese E.L., Dimitrakos T. and Turner M., Context-Aware Multifactor Authentication Based on Dynamic Pin, ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014, pp330-338
8. Damopoulos D. and Wetzel S., Introducing Research into the Undergraduate Curriculum in Cybersecurity, Information Security Education – 12th IFIP WG11.8 World Conference, WISE 12 Lisbon, Portugal, 25-27 June, 2019, pp30-42
9. von Solms S. and Marnewick A., Identifying Security Requirements Body of Knowledge for the Security Systems Engineer, – 12th IFIP WG11.8 World Conference, WISE 12 Lisbon, Portugal, 25-27 June, 2019, pp30-42
10. Thing V.L.L. and Chua Z.L., Smartphone Volatile Memory Acquisition for Security Analysis and Forensics Investigation, Security and Privacy Protection in Information Processing Systems - 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July8-10, 2013, pp217-230
11. Agarwal M., Puzis R., Haj-Yahya J., Zilberman P. and Elovici Y., Anti-forensic = Suspicious: Detection of Stealthy Malware that Hides Its Network Traffic, ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC2018, Poznan, Poland, September 18-20, 2018, pp216-230
12. Dupont G., dos Santos D.R., Costante E., den Hartog J. and Etalle S., A Matter of Life and Death: Analyzing the Security of Healthcare Networks, ICT Systems Security and Privacy

Protection - 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21-23, 2020, pp355-369
13. Yoo H. and Ahmed I., Control Logic Injection Attacks on Industrial Control Systems, ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, pp33-48
14. Vossaert J., Lapon J., De Decker B. and Naessens V., Trusted Computing to Increase Security and Privacy in eID Authentication, ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014, pp485-492
15. Eckel M., Fuchs A., Repp J. and Springer M., Secure Attestation of Virtualized Environments, ICT Systems Security and Privacy Protection - 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21-23, 2020, pp203-216
16. Kitkowska A., Shulman Y., Martucci L.A. and Wästlund E., Facilitating Privacy Attitudes and Behaviors with Affective Visual Design, ICT Systems Security and Privacy Protection - 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21-23, 2020, pp109-123
17. Simonet J. and Teufel S., The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users, ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, pp194-208
18. Rios R., Nuñez D. and López J., Query Privacy in Sensing-as-a-Service Platforms, ICT Systems Security and Privacy Protection - 32nd IFIP TC 11 International Conference, SEC 2017, Rome, Italy, May 29-31, 2017, pp141-154
19. Chen W., Lin Y., Galpin V., Nigam V., Lee M. and Aspinall D., Formal Analysis of SneakPeek: A Data Centre Attack and Its Mitigations, ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC2018, Poznan, Poland, September 18-20, 2018, pp307-322
20. Adepu S. and Mathur A., Using Process Invariants to Detect Cyber Attacks on a Water Treatment System, ICT Systems Security and Privacy Protection - 31st IFIP TC 11 International Conference, SEC 2016, Ghent, Belgium, May 30 - June 1, 2016, pp91-104
21. Drozd O. and Kirrane S. Privacy CURE: Consent Comprehension Made Easy, ICT Systems Security and Privacy Protection - 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21-23, 2020, pp124-139
22. Paul N., Tesfay W.B., Kipker DK., Stelter M. and Pape S., Assessing Privacy Policies of Internet of Things Services, ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC2018, Poznan, Poland, September 18-20, 2018, pp156-169
23. Caelli W.J., Kwok L. and Longley D., Evolving a Secure Internet, Security and Privacy Protection in Information Processing Systems - 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July8-10, 2013, pp217-230, pp42-54
24. Wheeler J.A., 2017, Top 10 factors for integrated risk management success, Gartner, Inc., https://www.gartner.com/en/documents/3645368/top-10-factors-for-integrated-risk-management-success, last accessed 16/12/2020
25. World Economic Forum (WEF), 2016, Digital transformation of industries: Digital enterprise, World Economic Forum white paper, http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/digital-enterprise-narrative-final-january-2016.pdf, last accessed 16/12/2020

26. Connolly L., Lang M. and Tygar J.D., Investigation of Employee Security Behaviour: A Grounded Theory Approach, ICT Systems Security and Privacy Protection - 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, pp283-296
27. Tolah A., Furnell S.M. and Papadaki M., A Comprehensive Framework for Understanding Security Culture in Organizations, Information Security Education – 12th IFIP WG11.8 World Conference, WISE 12 Lisbon, Portugal, 25-27 June, 2019, pp143-156
28. Cybersecurity Ventures, Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally By 2021, https://cybersecurityventures.com/jobs/, last accessed 16/12/2020
29. CSEC. Cybersecurity Curricula 2017 – Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Version 1.0 Report 31 December 2017. CSEC2017 Joint Task Force - Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf, last accessed 16/12/2020
30. Hui, K.L., Vance, A., Zhdanov, D. Securing Digital Assets. In: Bush A., Rai, A. (eds.) MIS Quarterly Research Curations, http://misq.org/research-curations, May 27, 2016. doi: 10.25300/05272016