This is the first issue of the SERENE-RISC digest, a quarterly publication from the SERENE-RISC Smart Cybersecurity Network.

SERENE-RISC uses a multidisciplinary approach to Cybersecurity Knowledge Mobilization by bringing together academics in the fields of computer and social sciences, as well as public and private partners.

The SERENE-RISC Quarterly Knowledge Digest is a distillation of research related to the securing and strengthening of Canadian cyberspace. It provides an update on academic research that can be understood at a glance, a skim or a quick read depending on your need.

The SERENE-RISC digest shares answers to questions from the latest research. These answers are then expanded in briefs that can be understood in 2 minutes. A 'one-pager' summary for each article follows to provide greater detail on the research and its outcomes. Each of these pages finishes with a very short take away message.

This document will be provided quarterly to SERENE-RISC members electronically (in PDF). Please fill out the membership application if you have not already done so to be a part of the membership group and receive this document on a regular basis to stay up to date on the latest Cyber Security Research in Canada and around the world.


serene risc Digest Autumn • 2014

Cutting Edge Research Summaries for Policy Makers and Practitioners

After a data breach, is it more costly to release credit cards right away or only release if there is attempted fraud ?

If only direct costs are considered, reissuing all affected cards appears more expensive than addressing fraud.

Can we make secure password management tools that people will actually use ?

Users recycle passwords, record passwords for later reference, and choose log in information linked to the context. These common strategies can inform software design.

Can I check if you are where you say you are online ?

Client Presence Verification (CPV) is a geolocation process that does not rely on information from the client, so can provide a reasonably reliable verification.

Do people actually change because of fraud and identity theft ?

People will be motivated to change their behaviour if they perceive some continuing risk.

Is it possible to usefully link different online accounts and still have privacy ?

By developing a common protection model for shared content, social computing systems can ensure user privacy and also the integrity of the privacy policy.

Do smart meters change security for Canadian energy providers ?

Yes, the technology requires a focus on resident privacy and data security on metering networks.

Can you tell a good IT security management tool interface from a bad one ?

Using a simple set of heuristic principles to assess management can highlight interface issues.

What good is just hitting about security problems ?

Social interactions that touch on security can raise awareness, motivation, and knowledge about practices and tools. This heightened sensitivity can influence individuals to change behaviours.

What is the fundamental step in securing critical infrastructure communications ?

The resilience of smart grids can be improved with the right configurations and settings for authentication protocols.

Do we really walk the talk of information security incident management standards ?

Actual practice is well aligned with recommendations, although some principles appear more difficult to implement in real life situations.

www.serene-risc.ca

serene risc Digest Autumn • 2014

Cutting Edge Research Summaries for Policy-Makers and Practitioners

After a data breach, is it more costly to reissue credit cards right away or only reissue if there is attempted fraud ?

The costs and benefits of different responses to credit card data breach are spread over cardholders, card issues, and merchants. This study compares the combined impact of automatically reissuing the potentially exposed cards and delaying card reissue until after an attempted fraud. The assessment model is based on several estimates - extrapolations of the total number of credit card records exposed in data breaches, the probability that a card exposed in a breach will be used for fraud, and the cost of fraud. The study indicates that if only direct costs are considered, re-issuing cards after a data breach is more expensive than waiting for an attempted fraud, but indirect costs shift the balance in favour of proactive re-issuing.
Credit card issuers can evaluate their own policy in light of the various factors presented in the model – the first and second-order costs, as well as the parameters used to assess the impact.

Do smart meters change security for Canadian energy providers ?

21st century Smart Grids integrate the advantages provided by Information Technology, but also the disadvantages. Currently in use in Canada is Advanced Metering Infrastructure connects that smart meters to utility management systems with bidirectional communication. New metering technology provides greater information for power management but also creates new security issues. User Privacy, Data Security and Cyber attack are added to existing issues of physical attacks and power theft. Standards and guidelines are in place for each of these areas however the combination of threats for advanced metering infrastructures appear distinct and requires special attention is required to address the new risks of this technology.

Can we make secure password management tools that people will actually use ?

To manage a high volume of accounts, users select log in information to reduce the burden of designing and remembering unique passwords; however, some of the often-used strategies compromise online security. Common habits include reusing passwords across different accounts, selecting passwords using algorithms or personal information, linking username and password for easier recall, and writing down passwords for later reference sometimes in easily accessible – and sometimes physically insecure – locations. The results of this research can be used to inform the design of realistic password management tools. The findings demonstrate that users are striving to follow advice about password security, but also budgeting the investment of energy across many accounts. To capitalize on this effort, new tools can improve on the coping strategies that people already use, for example single sign on, proving physically secure options for storage of password reminders, cues to remind the user of their password, and password management software.

Can you tell a good IT security management tool interface from a bad one ?

Usability is an important characteristic of Information technology security management (ITSM) tools, although there is little consensus on how to evaluate the usability of these resources. For this study, Jaferian et al. developed criteria for evaluating the usability of tools that support ITSM. The criteria take the form of a set of principles rather than fixed evaluation measures. These principles – or heuristics – describe common properties of usable interfaces, phrased in language that is easy to understand and open to interpretation. General rules such as these can prompt evaluators to find problems a user might encounter in a real world context. This study demonstrates that it is possible to evaluate the usability of ITSM tools and - given that severe problems with usability can be identified and addressed – this process is important to effectively supporting ITSM.

Can I check if you are where you say you are online ?

In order to tailor services by geography, web content and service providers may need to know the location of customers. This article proposes a new method to test the location asserted by the client. Client Presence Verification, or CPV, uses the location of three signals, called verifiers, which form a triangle in the vicinity of the client's claimed location. Each verifier sends messages to the client in question and measures the speed of response to each of the three corners of the triangle. By measuring the delays in responses and forwards, compared with the expected delays for the geographic distance and the traffic in that region, the verifiers can identify false assertions about client location. Although the multiple sampling technique is useful for reducing the effect of outlier measurements, the researchers established that the accuracy was not significantly improved past 100 iterations. The algorithm has some tolerance for error, in order to account for possible congestion and other things that might increase the delay. CPV could be used to verify client location with greater reliability than commonly used methods that rely on client information.

Do people actually change because of fraud and identify theft ?

This study simulated the scenario of fraud or identity theft by providing participants with a letter from a bank, describing how their personal banking information was compromised. Participants were asked to predict how they might react to the situation in real life, so that researchers could consider how reactions might differ with the circumstances detailed in the letter. The individual's perception of risk influences the motivation to change behaviour. This study provides insight into what reactions can be expected from people who are told about fraud or identity theft. Banks can use information about victims' responses in designing communication for fraud notification. If the purpose is to ease clients potential concerns, the message could provide different details, such as reassurance about the resolution, than if the objective is to motivate action, for example emphasizing unknown outcomes or risk to the individual in question. Where the underlying situation of fraud or identity theft is the same, victims are likely to react differently based on the information provided. When notifying clients about fraud or identity theft, financial institutions can use insight about what influences individual perception of risk to better motivate behaviour change.

What good is just talking about security problems ?

To understand why people might not be fully exploiting tools for online privacy and security, Das et al. elaborate on the idea that people base their decisions on understandings of how other people act to protect online privacy and security. Security sensitivity can determine behaviour change in adopting privacy and security tools. Interactions with other people can influence this sensitivity and thus contribute to changing behaviour. People reported talking about online security and privacy when a security threat or security tool was observed in action, such as when someone used a password function on a device. The findings also reveal something of the intent of social processes, which are often to warn others about a threat, to solve a presenting problem or share a solution. Privacy and security tools could be designed to take advantage of the social learning that occurs when people observe security behaviours of their peers.

What is the fundamental step in securing critical infrastructure communications ?

Critical infrastructure, essential assets for social and economic functioning, are increasingly linked into smart grids with computer intelligence and networking capabilities. This increased connectivity opens critical infrastructure to additional vulnerabilities, which can be managed with enhanced network security to minimize the threat of any potential cyber attack. In this study, Schukat discusses methods for improving the resilience of ICT in critical infrastructure, elaborating on settings and configurations for public-key infrastructure (PKI) and authentication protocols. When set with the right configurations, public key infrastructure and authentication protocols can improve the resilience of critical infrastructure against common cyber attack strategies.

Is it possible to usefully link different online accounts and still have privacy ?

For sharing content across social computing sites, many users connect multiple accounts. This generates challenges for the administration of privacy policies in that content might be posted to one site but accessed through another – how can the privacy policy guaranteed by the original site be applied across other platforms? The authors examined this issue to develop a protection model for shared resources, by evaluating options for Secure Multiparty Computation. Private Function Evaluation provides a method for keeping policies hidden to protect information about the site and users. Default policies for shared content, in contrast, can be publicly available; this approach can be combined with other technologies that mask the user and SCS inputs to provide privacy. These forms of Secure Multiparty Computation can be used to protect the content that is shared across social computing sites. This method safeguards both user information and the protection states of the SCS.

Do we really walk the talk of information security incident management standards ?

Organizations can plan for an effective response to information security incidents. Several tools exist to support this effort, including the recommendations of the International Standards Organization (ISO) for information security incident management. Tøndel et al. compare what is presented as good practice from articles that explore real experiences, with the recommendations from the ISO, to suggest where actual practice might align with, or diverge from, the ideal case. The findings provide an overview of the strengths and challenges in information security incident management as a whole. In addition the authors identify instructive examples of some key principles that can contribute to resilience in information security incidents. The results of the study suggest that the recommendations of the ISO regarding information security incident management are largely feasible.

Should Payment Card Issuers Reissue Cards in Response to a Data Breach?

In response to a data breach, credit card issuers choose between a) automatically reissuing the potentially exposed cards and b) delaying reissue until after an attempted fraud. Each option brings both costs and benefits spread across various contributors. In this study Graves et al. develop a model for comparing the relative merits of the two options, taking into account the total societal cost – that is, the combined impact on the time and finances of cardholders, card issuers, and merchants.

Data are compiled from several sources, including surveys and publicly available information about the extent of data breaches and credit card fraud in the United States. Since none of the information sources provides a comprehensive and precise value for any of these variables, the model is based on several estimates - extrapolations of the total number of credit card records exposed in data breaches, the probability that a card exposed in a breach will be used for fraud, and the cost of fraud. As a result, each of the input values is, in fact, a set of parameters – or a range of possible values – to reflect the potential variation. For example, anywhere between 2.5 to 40 million credit card numbers are exposed per year, of which 5 to 15% of numbers were obtained in data breaches.

The main model focuses on direct costs – the time and money invested in re-issuing cards versus remediating fraudulent use. If only direct effects are considered, reissuing all affected cards is more expensive than addressing fraud. This model demonstrates three potential indirect costs. The first occurs if card issuers decline to reissue cards automatically, breached data has a higher value to thieves, creating an incentive, because the data remains valid and can be used for fraud. Secondly, the time window for fraud is extended. Delayed fraudulent activity will be harder detect and more difficult to attribute to a particular data compromise. The third indirect effect concerns cardholder expectations; cardholders may perceive some increased risk of credit card use and thus choose other payment options. The reduced revenue for lenders would be an added cost of not reissuing cards. When the model includes these indirect effects the cost of waiting for an attempted fraud is greater than the cost of reissuing cards.

This approach is constrained by several issues including minimal, incomplete, inconsistent information. In extrapolating based on the known extent of fraud due to data breach, the authors highlight several ways the data for such studies might be improved, including more clear coverage of how credit card information is compromised. With their own more precise information about the extent of fraud from data breaches, credit card issuers might re-evaluate the parameters used in the model to determine whether the findings about relative costs will hold true for their situation.

Even the best available data leaves a wide range of uncertainty so the authors stop short of an assertive conclusion about which is more costly. A central implication of the findings is the impetus to look for more comparable data about the extent and mechanisms of data breaches. Credit card issuers may be well accustomed to assessing some of these costs to business; the model developed in this research suggests credit card issuers could also consider indirect costs of incentives, increased fraud windows, and cardholder expectations.

Card Issuers should analyze the intangible costs of not issuing cards on a breach before making a policy decision.

Graves, J., et al. (2014). Should Payment Card Issuers Reissue Cards in Response to a Data Breach? Workshop on the Economics of Information Security, Pennsylvania State University.

A survey on Advanced Metering Infrastructure

For many years utility providers have been concerned about power quality and the economy of the power system; however, 21st century technologies such as Smart Grids (SG) have brought new challenges of security and privacy of information. Smart Grids modernize electrical grids with Information Technology to maximize the efficiency and reliability of the system. This paper introduces the Advanced Metering Infrastructure (AMI) technology and its current status as the foundation of SG, which is responsible for collecting all the data and information from loads and consumers.

In Ontario, Canada, as one of the pioneers in AMI deployment, 4.7 million Smart Meters have been commissioned and 3.8 million Ontarians were being billed on Time Of Use system as of February 2012. AMI is a configured infrastructure that includes Smart Meters, Meter Data Management Systems, extended function software, and communication networks. Smart Meters communicate bi-directionally, sending meter data and accepting commands from the power supply network and can form home area networks providing more functionality or intelligent sub-metering for multi-tenanted residences. At the provider end, the system should store and analyse the data for billing purposes as well as managing demand response, consumption profiles, and real-time reactions to events in the grid.

AMI power grids represent a new security challenge as user privacy and cyber attacks are added to the existing issues of physical attacks and power theft. Smart Meters are capable of collecting information with higher frequencies than conventional meters with manual collection. Current technologies even allow for measurements every minute. Initial AMI projects deployed in Ontario sustain readings at intervals of 5 to 60 min.

By analysing Smart Meter data, it is possible to perform "consumer profiling" with an alarmingly high accuracy such as the number of residents, duration of occupancy, type of appliances, and security systems. By profiling usage it is also possible to identify resident behaviour and more with only 15-minute measurement intervals. Security is consequently significantly different with AMI to conventional meters.

The privacy implications of AMI will be better understood as it becomes more common. The governance of smart grid data collection is currently being discussed. In Canada, the Information and Privacy Commissioner of Ontario has issued relevant guidelines. These guidelines include the following seven "Privacy by Design" principles aimed at ensuring freedom of choice and personal control over one's information, as well as gaining a sustainable competitive advantage for organizations:

1. Proactive not Reactive Privacy (build privacy into goals)	2. Privacy as the Default
3. Privacy embedded into design	4. Full function & Privacy (win-win Solutions)
5. End-to-End Security	6. Visibility and Transparency
7. Respect for User Privacy	

To mitigate the risk of cyber-attack AMI power grids should implement measures to ensure information confidentiality, integrity, availability, and accountability, however the distributed nature of the network presents unique challenges. The threat of power theft has changed as AMI overcomes meter weaknesses but increases the risk of data tampering, as data is now vulnerable when stored and transmitted as well as at collection. These new forms of risk may require specific efforts as the standard approaches to security from either power or computing are not entirely well suited to securing AMI. For example, controlling physical access is impossible as meters are generally installed in insecure locations, the privacy solutions are retroactive and often zero-sum on an augmented system of coordinated security policies across interconnected systems with different stakeholders and interests. AMI is becoming established in Canada and adapting to new security challenges is of key importance to its success.

Advanced metering infrastructure use is expanding in Canada. Energy providers should address the added risks concerning customer data privacy, data security and cyber attacks.

Rashed Mohassel, R., Fung, A., Mohammadi, F., & Raahemifar, K. (2014). A survey on Advanced Metering Infrastructure. International Journal of Electrical Power & Energy Systems, 63, 473-484.

The password life cycle: user behaviour in managing passwords

Many users do not fully understand and exploit the available tools but do employ a range of strategies to manage online identities. To manage a high volume of accounts, with varying password complexity requirements, and often the need for frequent sign-on, users select log in information to reduce the burden of designing and remembering unique passwords; however, some of the often-used tools and tricks compromise online security. This study proposes that once identified, common strategies for designing, reusing, and recording passwords can be used design more appropriate password management tools. New tools might build on these existing patterns, channelling users into more secure practices.

The study is based on interviews with 27 individuals about use of passwords and use of tools such as password managers. Interviewers used screenshot images of various situations as visual prompts to encourage reflection on real-life habits. Based on individuals' accounts of their own password managing behaviour, Stobert and Biddle develop a model of the strategies people use in creating, remembering, and reusing passwords. Common habits include reusing passwords across different accounts, selecting passwords using algorithms or personal information, linking username and password for easier recall, and writing down passwords for later reference sometimes in easily accessible – and sometimes physically insecure – locations.

The authors found that these activities reflect careful systems of adapting, to ration the cognitive resources required to manage online identities and accounts. Although non-expert users do not always fully grasp the security risk that might be posed by their habits, their password managing efforts reflect a rational intent to handle the challenge of multiple passwords. Respondents report engaging more than one approach, in a way that often reflects a personalised strategy. In creating and committing passwords to memory, users are prioritising the security of some passwords at the expense of others. For example, by reusing or writing down passwords for lower priority accounts, users can conserve their energy for creating and remembering unique passwords for purposes with greater importance.

The results of this research can be used to inform the design of realistic password management tools. The findings demonstrate that users are striving to follow advice about password security, but also budgeting the investment of energy across many accounts. To capitalise on this effort, new tools can improve on the coping strategies that people already use, for example single sign on, proving physically secure options for storage of password reminders, cues to remind the user of their password, and password management software.

Users have password strategies based on assessed risk; password tools and policies would be better if they strengthened these tactics rather than dismissing them.

Stobert, E. and R. Biddle (2014). The password life cycle: user behaviour in managing passwords. Symposium on Usable Privacy and Security (SOUPS), Menlo Park, CA.

Heuristics for Evaluating IT Security Management Tools

Information technology security management (ITSM) tools support a number of goals, such as protection of networks and data, detection of threats, and management of users and their access. Because of this breadth of activity, ITSM involves technical complexity, as well as requires collaboration and information sharing among diverse stakeholders. Usability is an important characteristic of ITSM tools, although there is little consensus on how to evaluate the usability of these resources.

For this study, Jaferian et al. developed criteria for evaluating the usability of tools that support ITSM. The criteria take the form of a set of principles rather than fixed evaluation measures. These principles – or heuristics – describe common properties of usable interfaces, phrased in language that is easy to understand and open to interpretation. General rules such as these can prompt evaluators to find problems a user might encounter in a real world context.

The heuristic tool is developed from a review of literature on usability and real world problems with ITSM tools. These problems were then interpreted in light of a theory of human activities. After combining similar issues according to the theory, 7 heuristics for evaluating ITSM prevailed, each of which is supported and elaborated by more specific ideas.

This set of seven, listed below, form the proposed tool for evaluating usability of ITSM:

Heuristic	Short description
Visibility of activity status	Provide an awareness of activity in the context of time and space without unnecessary information
History of actions and changes on artefacts	Provide logging, auditing and reporting of historical user activity, policy changes, file access.
Flexible representation of information	Allow flexible report generation to suit different target audiences and tasks
Rules and constraints	Promote ITSM norms and rules while encouraging freedom of activity and choice within constraints
Planning and dividing work between users	Facilitate role delineation and work sharing between internal and external parties for programmed and ad-hoc work processes.
Capturing, sharing, and discovery of knowledge	Promote the capture, storage, and sharing of knowledge
Verification of knowledge	Provide for the safe and open validation and documentation of new tools and processes.

To evaluate the usability heuristics 28 participants applied the tool to various scenarios describing ITSM situations. Some of the participants used the ITSM heuristic tool, while others used a heuristic tool designed by Nielson that is commonly used in other domains of human computer interaction. The results of evaluations that were supported by each tool were compared. When compared with the Nielson tool evaluations, uses of the ITSM tool identified more problems and more severe problems, and also led to fewer false positives (such as problems that appeared to be usability concerns but in fact stemmed from technical constraints of the program).

The Nielson heuristics led evaluators to find additional issues not identified with the new tool; given this, a combination of the heuristics may be appropriate in order to evaluate ITSM usability. There is a correlation between the evaluators' number of years experience in Human Computer Interaction with the number of problems reported, but not with the severity of problems identified. Although an evaluator with more experience may be able to point out a higher number of problems, identifying potentially serious issues with usability may something non-experts can support.

This study demonstrates that it is possible to evaluate usability of ITSM tools and - given that severe problems with usability can be identified and addressed – this process is important to effectively supporting ITSM.

There are a few things you can check when trialling a tool interface that will pick up most of the big problems.

Jaferian, P., et al. (2014). "Heuristics for evaluating IT security management tools." Human–Computer Interaction 29(4): 311-350.

Location Verification on the Internet

In order to tailor services by geography, content and service providers that operate over the internet may need to know the location of customers. This might be necessary, for example, in order to comply with privacy regulations that vary across jurisdictions, to enforce licencing requirements that limit the availability of some services or content in some regions, or as a fraud prevention strategy. An adversary can undermine several commonly used methods for reading client location, by manipulating the Internet Protocol (IP) address or hiding the IP address for example by using a Virtual Private Network (VPN) or proxy. This article proposes a new method, termed Client Presence Verification (CPV), to test the location asserted by the client.

The underlying idea of CPV is to test the assertion of the client based on the relative position to three known points. CPV uses the location of three signals, called verifiers, which form a triangle in the vicinity of the client's claimed location. Verifiers are trusted sources, such as dedicated servers for location verification or any signal that is publicly reachable by internet. Each verifier sends messages to the client in question and measures the speed of response to each of the three corners of the triangle. By measuring the delays in responses and forwards, compared with the expected delays for the geographic distance and the traffic in that region, the verifiers can identify false assertions about client location. If, extrapolating from the known location of the three verifiers and the hypothetical sides of the triangle, the client location does not seem to fit within the triangle the provider can further investigate the validity of the location assertion.

CPV was tested using 2447 clients and 34 triangles of different sizes in the US and Canada. Based on 600 iterations of probing messages for each client, conducted over a one-month period, the investigators evaluated the accuracy of their method. In the sample, the probability of a false reject is 2% and of a false accept is 1.1%; out of every 100 clients that are legitimately located within the triangle, two may be falsely judged as adversaries. For every 100 adversaries, one will mistakenly be judged as a legitimate client. Although the multiple sampling technique is useful for reducing the effect of outlier measurements, the accuracy was not significantly improved past 100 iterations. The algorithm has some tolerance for error, in order to account for possible congestion and other things that might increase the delay.

A major advantage of CPV is the independence from information submitted by the client. There are ways of thwarting CPV, such as if an adversary delays the sending of response messages. However, this will only flag the client activity as fraudulent. Because a client cannot reduce the time involved in sending a message, they cannot manipulate the result of the CPV process; if a client is outside the triangle, the combined delays will be too large to match the expected regional delay. Given this, CPV could be used to verify client location with greater reliability than commonly used methods that rely on client information.

Triangulation based on data transfer speed can give a rough estimate on location; perhaps good enough to determine if a user is honestly representing their location or using proxies.

Abdou, A. M., et al. (2014). Location Verification on the Internet: Towards Enforcing Location-aware Access Policies Over Internet Clients. Conference on Communications and Network Security (CNS).

The Effect of Social Influence on Security Sensitivity

Tools are available to increase security, but are often not used to their full potential. To understand why people might not be exploiting these opportunities, research from various disciplines explores the factors that impact individuals' decisions about what to do and say to be secure. Building on this research, Das et al. elaborate on the idea that people base their decisions on understandings of how other people act. This study looks more closely at how social processes influence behaviour and communication related to security.

Previous research has found that several factors, known collectively as security sensitivity, can determine behaviour change in adopting privacy and security tools. Security sensitivity is the sum of awareness of threats and tools, motivation to use the tools, and knowledge of how to use the tools. Security sensitivity can be a barrier to adopting new behaviours and technologies, but can also drive change.

Nineteen participants took part in interviews, in which they were asked to recall recent changes to their use of security and privacy settings on various online media, and also to recall conversations about online security and privacy. In order to understand the context for those changes and conversations, interviews asked follow up questions about what catalyzed the changes. In particular, social catalysts – such as suggestions or warnings from friends – were distinguished from non-social catalysts – for example stemming from a personal negative experience or prompts from media reports.

Most people have experienced at least one change in behaviour or motivation driven by social learning. This suggests that sharing about privacy and security practices is already a common social process. There were specific reasons why people talk about online security and privacy. In many cases, a conversation surfaced when someone's privacy has been compromised, or when people shared ideas about how to use the features of specific systems. Conversations often arose when a security threat or security tool was observed in action, such as when someone used a authentication feature on a device. This observability was a key theme in exploring the context of conversations. The findings also reveal something of the intent of social processes, which are often to warn others about a threat, to solve a presenting problem or share a solution. The potential benefits of social learning about security are perhaps currently limited as individuals sometimes opt to keep quiet rather than risk appearing paranoid; there remains a stigma surrounding being too diligent with security features.

The design of social interventions to raise security sensitivity could capitalize on this social learning pattern. In particular, increasing the observability of tools and behaviours – while still preserving their privacy function – emerged as a promising avenue for leveraging the power of social influence. Actions that are observed become accessible for discussion, heightening security sensitivity, and conceivably the spread of security and privacy behaviours.

A good portion of what people know about security is learned from socialising and observation. Encouraging talk about security could be a good way of improving employee sensitivity to security issues.

Das, S., et al. (2014). The Effect of Social Influence on Security Sensitivity. Symposium on Usable Privacy and Security (SOUPS), Menlo Park, CA.

Behavioral Experiments Exploring Victims' Response to Cyber-based Financial Fraud and Identity Theft Scenario Simulations

This study simulated a scenario of fraud or identity theft by providing participants with a letter from a bank, describing a situation in which their personal banking information was compromised. Participants were asked to predict their own reactions. Researchers were interested in responses that reflected emotional reactions, perception of risk, any intention to change behaviour, and attitudes towards the role of government in cyber security.

The purpose of the experiment was to consider how people's reactions might differ with the circumstances detailed in the letter. For example, the researchers manipulated the information about the attacker; in some letters, the attacker was an individual, in others a group or an unknown entity. Some letters portrayed the attacker as motivated by fame, or by money, while others suggested the attack was carried out to finance terrorism. Other variables were whether the attack was resolved, unresolved, or uncertain; and whether the attack targeted a single individual's account or the entire bank database. The reactions to the different scenarios are compared to explore how different characteristics influence victim response.

Some circumstances are more likely to motivate victims' engagement. If the situation is unresolved or the outcome is unknown, and therefore may pose some recurring risk of harm, participants reported a stronger impetus to change their circumstance than if the situation is resolved. Intended behaviour change included such actions as discontinuing online transactions or purchasing an identity theft protection service. If the fraud was motivated by financial gain, victims are also more likely to perceive an ongoing risk than if supporting terrorism or some unknown objective was behind the attack. Victims report more motivation when their own individual account information is compromised, compared with the whole bank database; in this situation, victims are also likely to expect banks to increase security measures.

The individual's perception of risk influences the motivation to change behaviour. Different demographic groups tend to perceive risk in different ways, and a few demographic characteristics were examined in this study. Female victims are more likely to perceive risk and support government involvement, more likely to intend to seek help and invest in an online identity protection service. Similarly older victims are more likely to be emotionally engaged and to support a government response for cyber security.

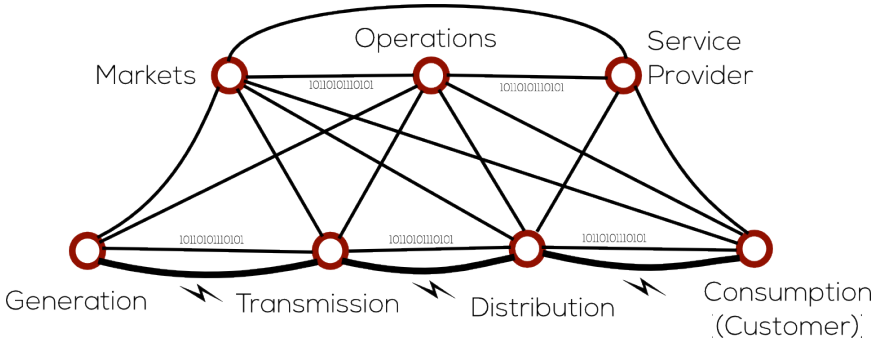
This study provides insight into how people respond, what can be expected from people who are told about fraud or identity theft. Banks can use information about victims' responses in designing communication for fraud notification. If the purpose is to ease clients potential concerns, a message providing details on the outcome or resolution of the breach would be appropriate. If the objective is to motivate action, notification focusing on the continuing risk to the individual may be more effective. Where the underlying situation of fraud or identity theft is the same, victims are likely to react differently based on the information provided.

People react to different security messages in very different ways and consider the attacker and motivation before changing their behaviour. Tailored notification for fraud may have more positive responses.

Rosoff, H., et al. (2014). Behavioral Experiments Exploring Victims' Response to Cyber-based Financial Fraud and Identity Theft Scenario Simulations. Symposium on Usable Privacy and Security (SOUPS), Menlo Park, CA.

Securing Critical Infrastructure

Critical infrastructure is made up of the assets essential for social and economic functioning, such as electricity, water, and transportation distribution systems. These resources are increasingly linked with computer intelligence and Information Communication Technologies (ICT) capabilities into smart grids. This ICT permits increased information flows between more actors – or end-points – and in more directions, expanding options for management of utilities. This increased connectivity opens the infrastructure to additional vulnerabilities, especially considering the limitations of smart grid components such as fixed computational resources, little or no user intervention once deployed, and placement in dispersed locations.



An integrated Smart Grid

In this study, Schukat discusses methods for improving the resilience of ICT in critical infrastructure. The suitability of ICT components is evaluated against a set of minimum standards for network security that, in combination, address the risk from common network cyber attack strategies. These standards are message confidentiality, message integrity, end-point authentication, and end-point authorisation.

Several settings and configurations can increase the resilience of smart grids against cyber attacks. These rely on public-key infrastructure (PKI) and authentication protocols. PKI involves a digital certificate that is issued and validated by third party authorities. The authentication protocol requires mutual authentication by peer end-points through a secure communication channel. Additional guidance is provided on how an authentication protocol can best support network security. The most applicable protocol is Transport Layer Security (TLS), which should be configured to require mutual authorizations by both end-points. Where TLS is not feasible, it might be possible to create something similar using other security appliances that act as a gateway between the end-point and network.

Other options include:

- Ensure Perfect Forward Secrecy (PFS) to protect against later compromise.
- Install a single certificate that integrates identity (public key) and attribute (permissions, rights) certificates.
- Provide multiple mechanisms for validating the status of certificates to accommodate situations when real time validation is unavailable.

Growing smart grids and interconnectivity of critical infrastructure reinforce the need to minimize potential damage of any possible cyber attack. Using knowledgeable settings and configurations for authentication protocols can contribute to network security.

Critical Infrastructure requires communications security; PKI, TLS and PFS provide a basic starting point.

Schukat, M. (2014). Securing critical infrastructure. The 10th International Conference on Digital Technologies (DT), IEEE.

On Protection in Federated Computing Systems

To take advantage of various unique services, users often create identities on multiple Social Computing Systems (SCS). To ease social sharing, many users connect multiple accounts to export content from one system to another (e.g. sharing recommendations from Yelp on Facebook). This generates ambiguities for the administration of privacy policies in that content might be posted to one service but accessed through another. This shared access is a challenge when protection policies may not perfectly match; how can the destination platform access and emulate the protection guaranteed by the originating platform, without breaching the privacy of the user?

Tarameshloo et al. examined this issue to develop a protection model for shared resources, by evaluating options for architecture and implementation of shared access policies. Secure Multiparty Computation (SMC) provides a method for access control policies that transcend the boundaries of any one SCS, and are enforced even after contents are migrated between systems. The practicalities are explored, including how a single shared policy can accommodate the different permissions applied on different services, using language that recognizes, honours, and integrates the terminology of different SCSs. SMC should achieve a fidelity of authorization and privacy policy, mechanism and states between services.

One of the challenges with SMC is the need to validate the privacy policy and access rights with exchange of information between the SCS, without disclosing either user information or details on the security policy of the SCS. The approaches to SMC of Private Function Evaluation (PFE) and Default Policies are evaluated in detail.
Under PFE, using distributed evaluation each SCS permits other SCSs to query their authorization mechanism to determine the sites protection states. A PFE protocol computes that shared access function in a secure manner, keeping private the inputs of each SCS. The table below contrasts the approaches to PFE architecture where either a shared content originator, user, or a third party is responsible for managing polices:

Architecture	Privacy	Knowledge of Query vocabulary	Fault Tolerance
Origin	Authorization decision should be hidden from origin SCS if it contributes an input to the policy formula	Every SCSs must understand the full query vocabulary of all other SCSs in confederation	Failing of one SCS affects all policy lookup of all resources originating from that SCS
User	There should not be any collusion between SCS	As Above	Failing of user storage will affect only the shared resources of that user
Third Party	Should remain trusted	Only Third Party must understand the full query	Single point of failure. Will affect entire confederation

The 'Default Policies' approach recognizes that most users will likely not independently specify a shared access policy for all content and so provides common and accepted standards. In this approach, SCS policies are not hidden, but rather publicly known. Each SCS determines whether the policies of other sites are trusted or not; in order to be deemed 'safe', the policy must ensure inputs are nondeducible – that is, they must remain private.

Secure Multiparty Computation can be used to protect the content that is shared across social computing sites. This method safeguards both user information and the protection states of the SCS. Both are desirable outcomes in a secure federated computing system.

Linking accounts online reduces security through dependency; mechanisms for determining the risk of a link can assist in managing the security of these arrangements.

Tarameshloo, E., et al. (2014). On Protection in Federated Social Computing Systems. Conference on Data Application Security and Privacy, San Antonio, Texas.

Information security incident management: Current practice as reported in the literature

Information security incidents are inescapable for most organizations. Anticipating this eventuality, organizations can plan for an effective response to information security incidents. Several tools exist to support this effort, including the recommendations of the International Standards Organization (ISO) for information security incident management (ISO/IEC 27035). The ISO recommendations organize activity into five phases: planning and preparation; detection and reporting; assessment and decision; responding; and learning.

Tøndel et al. conducted a systematic review of the published literature on real world experiences of information security incident management. They searched for all relevant articles and selected the highest quality studies; based on their criteria they identified 15 studies published after 2005. Each of the articles recounts the circumstances of an information security incident and subsequent incident management in a different organization. The sample represents a variety of types of organizations and also a range of research methods. The information security incident management experiences presented as good practice from these studies are compared with the recommendations from the ISO, to suggest where actual practice might align with, or diverge from, the ideal case.

A summary of the learning related to each phase of the ISO framework is presented (e.g. what is learned about the plan and prepare stage in particular) along with a synthesis of the strengths and challenges in information security incident management as a whole.

ISO Phase	Examples of identified practices:	Examples of practices more difficult to implement:
Planning and Preparation	Defining security incident and process for response	Promoting awareness about information security
Detection and Reporting	Providing automatic tools and manual reporting for detection	Documenting all incidents
Assessment and Decision	Confirming and classifying all incidents	Exercising caution in outsourcing situations
Responding	Automating and prioritizing responses	none identified
Learning	none identified	Evaluating each incident and disseminating information

Instructive examples of some key principles are identified, such as simple plans for incident management, automated processing for common and low-risk incidents, and tracking of and notification about incidents. For some components of incident management that remain unclear or appear to be untested, additional tools or guidelines could support tasks such as the classification of incidents, securing senior management commitment, involving all employees across an organization, and clarifying responsibility in outsourcing.

The recommendations of the ISO regarding information security incident management are largely feasible. Some challenges to implementation of information security incident management can be anticipated and even moderated or resolved in the design and roll out of incident management plans. Further, some examples are highlighted that might inspire action or inform specific practical action in planning and response. There are some gaps in real world practice of information security incident management that could be met with attention to planning and implementation.

Industry can follow the security standards but the standards aren't enough to keep industry secure.

Tøndel, I. A., et al. (2014). "Information security incident management: Current practice as reported in the literature." Computers & Security 45: 42-57.