TU Delft

Delft University of Technology

Change that Respects Business Expertise

Stories as Prompts for a Conversation about Organisation Security

Parkin, Simon; Arnell, Simon; Ward, Jeremy

DOI
10.1145/3498891.3498895

Publication date
2021

Document Version
Final published version

Published in
New Security Paradigms Workshop, NSPW 2021

Citation (APA)
Parkin, S., Arnell, S., & Ward, J. (2021). Change that Respects Business Expertise: Stories as Prompts for a Conversation about Organisation Security. In *New Security Paradigms Workshop, NSPW 2021* (pp. 28-42). (ACM International Conference Proceeding Series). Association for Computing Machinery (ACM). https://doi.org/10.1145/3498891.3498895

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

Change that Respects Business Expertise: Stories as Prompts for a Conversation about Organisation Security

Simon Parkin
Delft University of Technology
Delft, Netherlands
s.e.parkin@tudelft.nl

Simon Arnell
Configured Things Ltd.
Bristol, UK
simon.arnell@configuredthings.com

Jeremy Ward
Independent Researcher
Bath, UK

ABSTRACT

Leaders of organisations must make investment decisions relating to the security of their organisation. This often happens through consultation with a security specialist. Consultations may be regarded as conversations taking place in a trading zone between the two domains. We propose that supporting the trading zone is a route to sustainable, workable security change improvements. Prompts for such improvements are already in place, in the security stories that reach business leaders through news media, or anecdotes from trusted peers. However, a shift in perspective is needed to view these stories and anecdotes as prompts for individual decision makers to enter into the trading zone with security specialists. We illustrate how to facilitate this shift by recasting security ontology tools, previously centred around security-specific expertise, as a support device to enrich conversations between business expertise and security advice toward finding workable security choices. We frame our proposal within a broader view of community transformation, exploring the important principle of identifying practical opportunities to inform discussions about security solutions that are appropriate in the business context. Community-level discussions have potential to lead to more lasting, effective improvements than those instigated by one-way interventions from security specialists. We extend the view, applying the paradigm to articulate the importance of two-way conversations between business peers and security specialists.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; • **Applied computing** → Business-IT alignment; *Decision analysis.*

KEYWORDS

Cyber security management, security stories, security transformation

This work is licensed under a Creative Commons Attribution International 4.0 License.

NSPW '21, October 25–28, 2021, Virtual Event, USA
© 2021 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8573-2/21/10.
https://doi.org/10.1145/3498891.3498895

ACM Reference Format:
Simon Parkin, Simon Arnell, and Jeremy Ward. 2021. Change that Respects Business Expertise: Stories as Prompts for a Conversation about Organisation Security. In *New Security Paradigms Workshop (NSPW '21), October 25–28, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3498891.3498895

1 INTRODUCTION

Businesses are often urged to boost their cybersecurity capability, especially at a national policy level [7]. This can include investing in infrastructure to address new threats, and 'security hygiene' to limit commodity attacks, such as keeping software up-to-date on computers used for work activities. More nuanced advice addresses how to avoid social engineering attacks (such as phishing emails) – efforts to make such controls work in practice highlight that the context of the business must be taken into account to ensure that businesses are secure against online and digital technology threats.

Decisions about strategy are made or approved, at an executive level, by the leaders of the organisation. Strategic decisions increasingly include aspects related to cyber security. Organisations may receive messaging from bodies of expertise suggesting they need to do more to secure themselves and other organisations they work with. Pressure from such messaging is especially felt by smaller organisations [39].

That there can be pressure without support brings attention to a gap in the provisioning around advice to organisations: large organisations and those with regulatory expectations typically have a risk or governance function. These factors make security a board issue [13]. However, smaller businesses fall into the chasm of 'one size fits all' advice, which is generic and lacking in sufficient detail to enable them to address specific threats [56]. Further, for sole proprietor or micro businesses, the advice provided to them by expert bodies begins to overlap with the advice given to individual members of the public.

Critically, business leaders do not get their security information only from national policy-makers and training providers. They also hear about threats and new (security) technologies from peers and news articles [33]. Certainly, for members of the public, where a person gets their information from influences what they learn about security [43]. Whilst organisations required to comply with regulatory processes will have some form of governance apparatus; small business leaders may make security decisions as a result of fleeting conversations with acquaintances, based on stories they have heard or read in passing.

This brings us to consider the importance of security information, delivered to business leaders through stories from media sources, and informally communicated anecdotes, in helping to prompt timely business decisions. Previous research has shown that, whilst

stories are not as robust as facts and concrete advice, they can often inspire change [57]. Business leaders reaching out to security specialists with unqualified stories and anecdotes may be seen as an irritant [33], where interventions in this space can be seen to focus on qualifying the knowledge of the business leader first.

Here we posit that this interaction between business leaders and security, prompted by stories and anecdotes, should be seen instead as a valuable and dynamic meeting place where the areas of business and cybersecurity expertise can converge. Stories and anecdotes can become, in effect, a 'trading zone' [54] where both sides can bring their knowledge and experience to the conversation, around an artefact such as a news story, and engage in more meaningful and productive dialogue.

1.1 Our contribution

There is potential for stories about security to drive a change in individuals' personal security behaviours [44]. This includes stories from online and TV news [12]. Businesses, especially smaller ones, rely on conversations and prompts to take action. We explore the potential for reframing business leaders as actors who receive security prompts from both interactions with peers and from non-security news sources.

The idea that business leaders will go to security-focused news sources or dedicated sources of security advice rests on a precarious assumption, not only that these leaders know these sources exist, but that they dedicate time and thought to security as a standalone interest independent of their running of the organisation. We focus on the natural trading zone that occurs when a business leader acts on new information and consults a security specialist.

Rather than security-focused interventions which transform the recipient into more of a security expert, our proposal is to reframe tools of security intervention to instead support a meeting point between areas of expertise, as an opportunity for transformation. This acts as a bridge between business leaders (as context experts) and security specialists who they consult in order to address concerns. Our paradigm is built on the following:

- **A shift to respectful security change.** Characterising business related security stories, be they news stories or anecdotes, as a prompt for security change, recognises their role in the *trading zone* between business and security specialists. This represents a shift away from dismissing informal sources and conversations about security as inferior to security-focused advice from security experts; the latter requires business leaders to dismiss the trading zone that is valuable to informing strategic choices about security. We describe this shift in perspective through Section 2.
- **Creation of tools to support conversations, not edicts.** To support the interaction between business leaders and security specialists, we combine principles from both security knowledge-sharing tools and the sharing of security stories. We adapt aspects of existing security knowledge ontology tools which can be used to formalise information and relationships between concepts (e.g., [14]). This supports different perspectives in a shared pool of knowledge, rather than just the view steeped in security terminology. Section 3 describes our reframing of a security ontology tool, and Section 4 how the tool would be positioned to support the conversation about security where it is likely to happen.
- **Transformation support as distinct from security interventions.** Our approach embodies not only a retooling, but a valuable *process for change* that is distinct from typical security interventions, and better supports existing ad-hoc decision-making practices. This process is informed by the approach for community transformation described by Block [5], as applied to a range of community change projects. Businesses engage with peers, but also informal or formal associations of similar organisations, and communities of practice. A restoration of community *"acknowledges that we have all the capacity, expertise, and resources that an alternative future requires."* There is then an emphasis on supporting the opportunities in what businesses can drive themselves. We discuss several immediate possibilities in our Discussion (Section 5), consider Related Work (Section 6), and close with Conclusions in Section 7.

2 BACKGROUND

In this section we expand on the motivations for our work, shortcomings in current approaches to communicating secure working practices to organisations (more so smaller businesses), and characterise opportunities. We do so by first outlining various means used at nation-level to convey advocated cybersecurity practices to business. We then relate this to risk management in medium-size and smaller organisations which lack dedicated a security apparatus, leading to how good security practices can be encouraged in this context and the potential to leverage security stories.

2.1 Official means of communicating security to business

We summarise approaches at nation-level, which characterise the existing variety of recognised methods for communicating security advice (as may be used by governments and security services companies alike), using a limited number of region-specific example.

The UK NCSC (National Cyber Security Centre) signposts topic-specific advice for organisations. It also produces targeted materials, including a succinct Small Business Guide (adapted also as a guide for small charities), a 'Board Toolkit' aimed at business leaders, and toolkits for producing awareness campaigns and security games within an organisation. These materials point to basic steps to follow, and may be renewed at intervals, complemented by technology- or process-specific online pieces (as is seen in other nations). These materials are all made available via the NCSC's website, promoted as a central point for authoritative advice. Materials may then be communicated at gatherings of business representatives, etc. The UK also promotes "Cyber Essentials"[1]; these are basic security controls, which can be implemented and assessed locally by approved auditors.

In the UK, sole traders and self-employed workers are addressed by both the NCSC small business guidance and the advice for citizens (Cyber Aware)[2]. This, in a way, acknowledges that individuals – rather than regimented business processes – are driving security

[1] https://www.ncsc.gov.uk/cyberessentials/overview
[2] https://www.ncsc.gov.uk/cyberaware/home

in these smaller businesses. This is mirrored in Europe, where basic advice is signposted for businesses by ENISA[3], again via an online presence, and complemented by campaigns and initiatives (such as the annual European Cyber Security Month of workshops and other events to communicate advice more directly).

Regarding sharing of intelligence, the UK also has the region-specific Warning, Advice and Reporting Point (WARP)[4] initiative, where 'Information Security, Assurance and Governance practitioners' converge to exchange incident information and to discuss threats. Membership of these WARPs is largely confined to the public sector. There is also the Cyber Security Information Sharing Partnership (CiSP)[5], aimed at supporting confidential sharing of technical intelligence between businesses and within business sectors. The UK NCSC also provides technical advisories of new/emerging threats, intended for general consumption by organisations (albeit those who are aware of them) – similar initiatives are found elsewhere, such as in the Netherlands, coordinated by a similarly named NCSC, which is unaffiliated with the UK's NCSC.

Government-level cybersecurity guidance in the USA is generally mediated through the National Institute for Standards and Technology (NIST)[6]. Similar to the UK and Europe, NIST produces best practice advice and resources, but also develops technology-specific cybersecurity standards and guidelines (covering topics such as access control and IoT security). In connection with this mission is the National Initiative for Cybersecurity Education (NICE)[7]; with its accompanying cybersecurity framework for use in businesses and other institutions[8]. Various stakeholder groups seek to involve organisations and individuals in security-related education and advice[9], though as with initiatives elsewhere, 'communities of interest' here are drawn from individuals and groups with professional interest in cybersecurity and privacy issues. Specific sectors may have targeted advice, such as critical infrastructure which historically, and inherently, has had more support and guidance at a nation-level; specific technologies used in particular sectors may have more advice available.

2.2 Limits to the provision of advice by expert bodies

There are shortcomings to security advice aimed at an organisation level, similar to those around advice to individuals, such as an assumption that *"as long as citizens are aware of the risk, and are provided with information on how to improve their security behaviour, behaviour will change."* [56]. Historically, nation-level expert security advice focused on CNI first or only, and even where some countries are diversifying their advice to different sectors/organisations, lessons are still being learned about how to channel advice in an appropriate way.

Reeder et al. [46] identify challenges for communicating security behaviour advice (including how general or specific the advice is), but also dimensions by which to measure it, specifically whether it is effective, actionable, consistent, and concise. Although the work focuses on advice aimed at citizens, these dimensions can be considered in the scope of advice to Small-to-Medium Enterprise (SME) leaders as individuals. Little consideration is given by official sources (not just governments, but local municipalities and police forces, etc.) to the provision of security advice that is accessible, relevant and takes into account the business needs of SME leaders – all of these are assumed.

In terms of the support provided by external advisors and experts, organisations cannot solely be differentiated as either 'large' or 'small'. However, organisations with comparatively small resourcing or capacity are less likely to be able to afford and maintain advised solutions, and indeed may in some cases go the other way and run up 'security debt' by forgoing useful security controls for lack of resources [31]. In short, we regard as 'smaller' organisations those with limited resources and increased pressure to ensure that spending on security is effective. We also consider the diverse nature of IT systems in smaller organisations; general advice is less likely to match to their infrastructure needs [40]. However, some of the same security threats that affect large organisations may apply, such as opportunistic phishing attacks, and a need to keep commodity software up-to-date.

2.3 Managing security with(out) security management

Organisations wishing to implement their own security programmes typically need a dedicated security management team – this will come at a cost beyond the reach of most SMEs. SMEs may have only a single individual with designated security management duties, if that; instead, they may outsource IT and IT-security to an IT service provider, or approach a trusted IT advisor on an ad-hoc basis (for instance when looking for advice on purchasing or setting up new IT hardware). SMEs will therefore generally perceive specialised security products and processes as cost-prohibitive. This view can be justified by the fact that, whilst larger organisations are likely to have stringent regulatory or shareholder requirements which make a high degree of security oversight inevitable, SMEs are less likely to require such a level of dedicated security apparatus [33].

Threat intelligence (TI) is an aspect of cybersecurity which is of growing importance. Larger, more mature organisations will typically have their own internal capabilities in this area, such as TI teams operating within a Security Operations Centre (SOC) function. This facilitates proactive analysis of the context in which their organisation operates, gathering tailored intelligence to anticipate future attacks. Although there have been advancements in standardisation of Indicator-of-Compromise (IOC) interchange methods and automation of information sharing, such interchanges and sharing will be limited by the technical means and expertise available to participating organisations; and as such are likely to be beyond the reach of most SMEs.

This begins to highlight that, if security notifications are aimed at security specialists (e.g., technical vulnerability details, software versions, configuration options), and not at business leaders, they may miss their mark entirely. This is critical when even SMEs have certain basic security requirements that must be met as a result of

[3]https://www.enisa.europa.eu
[4]https://www.ncsc.gov.uk/information/what-warp
[5]https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
[6]https://www.nist.gov/cybersecurity
[7]https://www.nist.gov/itl/applied-cybersecurity/nice
[8]https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
[9]https://www.nist.gov/cybersecurity/cybersecurity-privacy-stakeholder-engagement

regulatory expectations (for example from the GDPR and payment card industry). The security guidance available to these organisations either tends to assume that baseline measures are already in place, or is unhelpful in clarifying and prioritising the actions needed to meet baseline control levels required by an individual organisation [38]. Since SMEs generally make up 99% of businesses [40], the provision of business-aligned security guidance for SMEs should be a top priority. In contrast to this, leaders of smaller businesses must be supported in a way which does not make excessive assumptions about their security knowledge. What can be leveraged is their knowledge of their own business and its priorities, which could be *affected* by security events.

Stories about security issues and data breaches can influence the level of support for investment in cybersecurity [33], in even those large organisations which use dedicated board meetings to discuss decisions and changes [30, 37]. Looking to industry surveys such as the UK's annual Cyber Security Breaches Survey [13], a majority of businesses seek external information or guidance relating to the security of their organisation. Where SMEs practice ad-hoc security investments, news stories become an important mechanism for prompting engagement with new advice.

2.4 Encouraging change and secure practices

There is a difference in the terminology in sources of information used by security specialists and non-experts [43]. The latter are seen to focus on the *who* of attackers and their motivations; sources of expert knowledge are noted to focus instead on the *what* of an attack vector, connecting attacks to protective measures. This highlights where best to leverage security specialist knowledge in the conversation about security, by drawing in those connections during a dialogue where both can contribute understanding to a more complete picture.

Business leaders are a distinct category of individuals, left underserved by these kinds of interventions. They are individuals, but they make decisions about an organisation, *their* organisation, informed by *conversations* which leverage new information that they receive. These decisions include investments and business strategies, but also responses to the risks they perceive in their business environment [52]. Larger businesses have structured risk management processes, and home computer users are broadly assumed for the most part to act within a limited ecosystem of operating systems and digital device interfaces. Most businesses fall somewhere in-between, but *crucially*, decisions are made by someone closer to the latter, for a context closer to the former. Plainly, business leaders are individuals (assumed non-security experts) who have to make a decision about new security information, relating investment and risk [3].

Not all businesses are the same, certainly when looking at smaller organisations with increasingly diverse digital infrastructure [39]. Smaller organisations such as SMEs also have more constraint on the resources they have available for security investments [3]. SME leaders then have to be careful about which controls they choose to implement, making an assessment from a view more of costs than efficacy, where a judgement on the latter may be made instead by a security specialist more knowledgeable than them. We posit here that stories about security are still useful for these leaders in their own business context, as a vehicle for the conversation with a security specialist, about how to tailor security to fit the organisation.

2.5 Stories inform security investment decisions

A well-placed *prompt* can activate a new behaviour [16]. According to the B=MAP persuasive design model, a Prompt can augment existing Motivation and Ability as a facilitator, spark, or signal toward a new behaviour. The potential for prompts to encourage improved security behaviours, including through interactions with peers, has been noted for individual home users [10].

A security-related news story or anecdote may be current, such as a recent security incident, e.g., a data breach or targeted network-based attack, or an anecdote that is told *"like one recently of a Solicitor who was tricked into transferring over clients' money"* [27]). If the story or anecdote mentions details about another business (the affected organisation) which are potentially relevant to a reader's own organisation (such as a similar sector, business activity, organisation structure, or digital infrastructure), it can act as a *signal* that there is a new piece of information to consider within the business strategy. The signal just has to be strong enough – relatable enough – to prompt a question of whether action is required to avoid threats mentioned in the story. The question encourages engagement with a security specialist, such that a prompt *facilitating* that engagement is key. At present, finding such signals is serendipitous, depending on stories that a business leader happens to read or is told about.

Social prompts can occur in different forms [10]. Here we consider these as social (e.g., told by someone else, such as a peer), forced (e.g., regulatory or supply chain requirements), or proactive (e.g., reading news). Where there is potential is that social and proactive prompts leverage activities which are naturally happening for most businesses – leaders also talk to peers [38] (who have social influence on others operating businesses [3]), and read news stories [33]. The *messenger effect* [6] that external interventions aim for is already present, as is the *salience* of news and anecdotes often being about topical events such as recent security incidents.

Where news stories often discuss pertinent incidents, government-level advice seldom changes, if at all, over time [56]. As a result, external advice and government or consultant interventions may have limited effects on smaller organisations [24]. For smaller businesses, having trusted services may be more effective than 'formality' [2] – the observation that 'serious lessons [from relatable stories] are retold' [44] then has more power.

Spring et al. [54] discuss 'trading zones' and the interactions of different domains of knowledge to address complex issues, as distinct from instead imposing a common language that both sides use. A business leader does not hear an anecdote or read a story, and immediately pay out for a control matching the incident described in the story. Existing security interventions achieve their success most readily by imposing a common understanding of security. However, organisation security is complex and security must be balanced with other imperatives. We see the conversation between a business leader and a security specialist as such a trading zone. Businesses may be on somewhat of a sliding scale here in terms

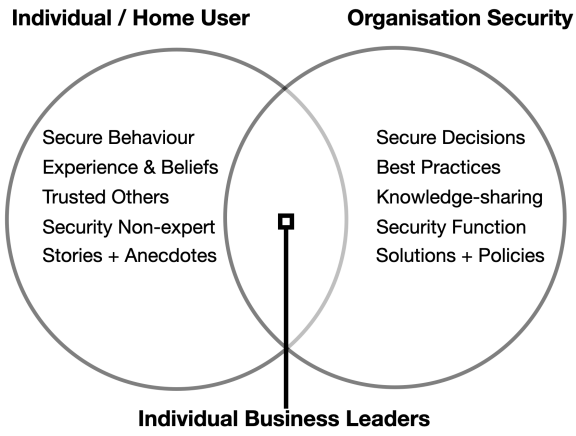

Figure 1: Business leaders are individuals, and responsible for decisions about the security of their organisation(s). We represent the qualities of Individuals and Organisation Security to each side of the diagram, with Business Leaders in the space between – the conversation between business and security expertise is a way to meaningfully bridge the two prominent areas of security intervention.

of how involved they are in the decision-making process, but it all happens in that conversation (even if the decision is to delegate the choice to the security specialist). We then have two sides to the conversation, with the trading zone between domains in the centre (as in Figure 1).

Business leaders do not necessarily manage the IT and security of their organisations themselves, and may employ a known expert or an IT provider. This again puts them somewhere between a home computer user and typical corporate-level risk management apparatus. One consequence of this is that where advice for home users ought to be actionable, improve security, and be comprehensible [45], for a business leader this assessment becomes collaborative. Just as Redmiles et al. consulted security experts to judge the efficacy of the advice they assessed [45], a business leader, or leaders, may approach a security specialist to assess whether a particular security control fits their business or would improve security [3], within investment constraints.

That security expertise is 'outside' of the decision-maker is one side of the story; a business leader reads a story or piece of advice, and comprehends it as *potentially* relevant to their business context (and so they need to *explore* that relevance rather than be told it). If there is no information in the advice that relates to that context, the opportunity is lost. This may be the case with more technical sources of security advice/information [43], while also considering that presenting security to business leaders as a full, unfamiliar, and daunting implementation could dissuade them [50].

2.6 Summary: supporting transformations

We propose an approach of encouraging both (i) prompts to have conversations (through delivery of support) and (ii) further empowering of the two domains of expertise to identify appropriate, lasting security investments relative to an organisation's risks. We explore delivery and positioning of this support in Section 4.

We envisage the support of conversations as a distinct option alongside existing intervention approaches, with a belief that this could be more effective as a long-term, respectful way to encourage improvements. Existing interventions have a particular change in understanding or adopted solutions in mind; we identify *transformation* as a possibility which is owned by the business community, with *potential* for change. We point to how this could open up new avenues in Section 5.

We challenge the presumption that 'informal stories' in the business sphere are of no value, or worse, dangerous. On the contrary, these are existing prompts which can boost their value when used as social sensitising factors [11] between professionals, and can be bolstered to improve their value. It can then become more a case of 'advisors helping businesses to do security in the right way', rather than 'advisors helping businesses to do security the advisors' way'.

To frame our approach, we build on the principles of community transformation described by Block [5]. We regard especially 'local' groups of smaller organisations/businesses each as a 'community', extending to the collection of smaller businesses at a nation level, and so on. Foremost, Block points out that if change relies on external experts to directly dictate how a community should conduct itself, it frames that community as a set of problems rather than *"a community of possibilities"* [5]. Block posits that community-driven change relies on the following foundations, which we adapt:

- **Accountability and commitment**, where business leaders *"will be accountable and committed to what they have a hand in creating"*.
- **Focus on gifts**, rather than on deficiencies. Business leaders arguably know their organisation and how to keep it running better than anyone else.
- **Trust** in the community to solve its own problems. Peers naturally share security lessons and stories, and choose whether to act on them. This points to positioning support appropriately to achieve this.
- **The power of language & context**, realised by having a conversation that *"we have not had before"*. We consider retooling to support exploration of options, rather than to drive businesses to meet external experts' expectations, as in Section 3.
- **Aliveness**, where Block frames this around the small steps. In this context, we regard this as giving consideration to where and how to accommodate the conversation about security. We explore this in Section 4.

These principles guide how we propose to support the trading zone as an effective vehicle for *transformation* rather than *intervention*. This is an approach which respects expertise where it already exists, utilising the trading zone between business and security knowledge toward identifying workable, sustainable security solutions. Foremost this addresses the concerns of business leaders who lack a fully-developed governance infrastructure, but who are nonetheless working to operate a business. Recognising the potential of this trading zone and that it exists (and is not something to 'wipe out and replace') is what empowers a sustainable community

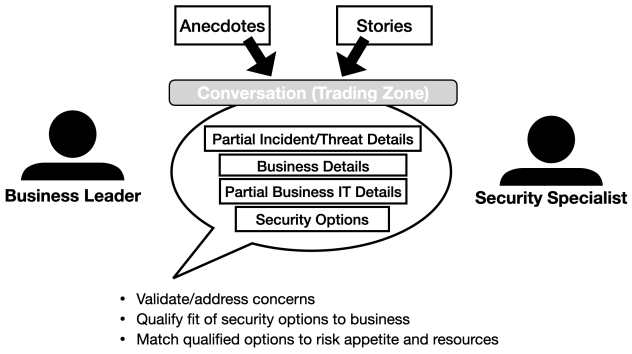

Figure 2: Elements of the conversation between business leaders and the security specialists they engage with, in pursuit of addressing (prompted) concerns initiated by (partial information within) news stories, or anecdotes from peers in other businesses.

transformation (rather than perpetually undermining its capabilities, and blocking change). Even for individuals, approaches to security can be *"complicated and situational"* [44].

3 RETOOLING FOR THE CONVERSATION

We propose to adapt the vehicle of a security knowledge ontology, where there are examples of ontologies in security elsewhere [14, 41]. Here we illustrate how the shift from interventions with high knowledge entry-costs where an individual must basically already know what they need to know [43]), to supporting opportunities for transformation through varied perspectives on security. Where we frame stories and anecdotes as the prompt for those opportunities, it is less preferable to have the conversation informed by (potentially) vaguely-recalled details. We frame the conversation and what each side brings to it in Figure 2, where this includes recognition that each side brings a part of the bigger picture, and that particular outcomes may be sought, such as validating concerns or finding solutions which address the business leader's concerns, or ideally, their organisation's needs.

3.1 Design principles

We will adapt security knowledge-sharing / ontology tools in a principled manner, to accommodate a respectful transformation of security. We define a set of design principles for the ontology as follows, though they may be applicable to other tools designed to support security change through community transformation:

- **Acknowledge decision complexity.** Recognise the expertise of the decision-maker, and the complexity – and compromises – in any decisions made about business security.
- **Explore solutions together.** Reconfigure intervention tools to support a conversation about possibilities. Information from peers usually focuses on the 'who' of an attack [43], information from news sources may elaborate on consequences, and expert sources examine further the 'how' on an attack – a non-complete set of details may be brought to the discussion, as in Figure 2. We focus on trust in the business community to make use of evidence once it is provided.
- **Inform rather than replace decisions.** Identify the prompt to explore a decision around security. Support the preparedness for making an informed decision with relatable information, rather than supplanting the decision with one-way expert advice which may *"miss its audience entirely"* [43].
- **Relate to beliefs.** Identify where the decision-maker interacts with security expertise, as a conversation. Rather than assuming to recast the decision-maker as a security expert in their own right, respect the difference between Security Thinking and Secure Behaviour [44]. The Security Thinking can include 'security beliefs' [58] which need to be checked during the decision-making process.
- **Support option discovery.** Identify and support existing modes of interaction between domains of business and security expertise, rather than disturb naturally-occurring opportunities for engagement with security. As such, be prepared for possibilities to take their own time. An ontology would also facilitate flipping around, or sharing, perspectives in a transparent manner, which is important when engaging with a *trusted* IT/security advisor. Not every security improvement has to be an intervention effected from outside. We broadly explore this in Section 4.

3.2 An ontology for a conversation

An ontology can be used to define a common vocabulary for use by members of a particular community of users [29]. An ontology comprises a set of concepts, relations, and axioms that formalize knowledge of interest. An ontology supports discussion of the response to pressing concerns about the security of an organisation, and encourages deeper questions, rather than imposing a flat 'here is what to do' approach. It also supports transparency in the examination of detail for making an informed decision around security solutions. Use of an ontology tool aligns with our design principles, as it can encode and link elements of terminology through explicit connections between disparate terms, as a common language between 'auras of understanding' [41].

Ontology content can also be re-purposed and refined. Reliance on an ontology presumes a means to formalise and logically connect elements of a conversation. It would be better approached as a point of reference that helps to relate different perspectives on security concerns, as relates to 'trading zones' in Section 3.6.

The ontology is shown in Figure 3, where overlaps are suggestive of common ground (if not common terminology). The overlap of domains is the central artefact of a security conversation, a news story or anecdote and a belief about how it relates to security. The ontology has been implemented in the OWL Web Ontology Language using Protégé[10], and is available at https://github.com/simonarnell/security-storytelling-ontology.

3.3 Ontology elements

The ontology design (Figure 3) is informed by the following incomplete list of elements which are useful to include, as informed by prior research in infromation security risk management ontologies

[10]https://protege.stanford.edu/

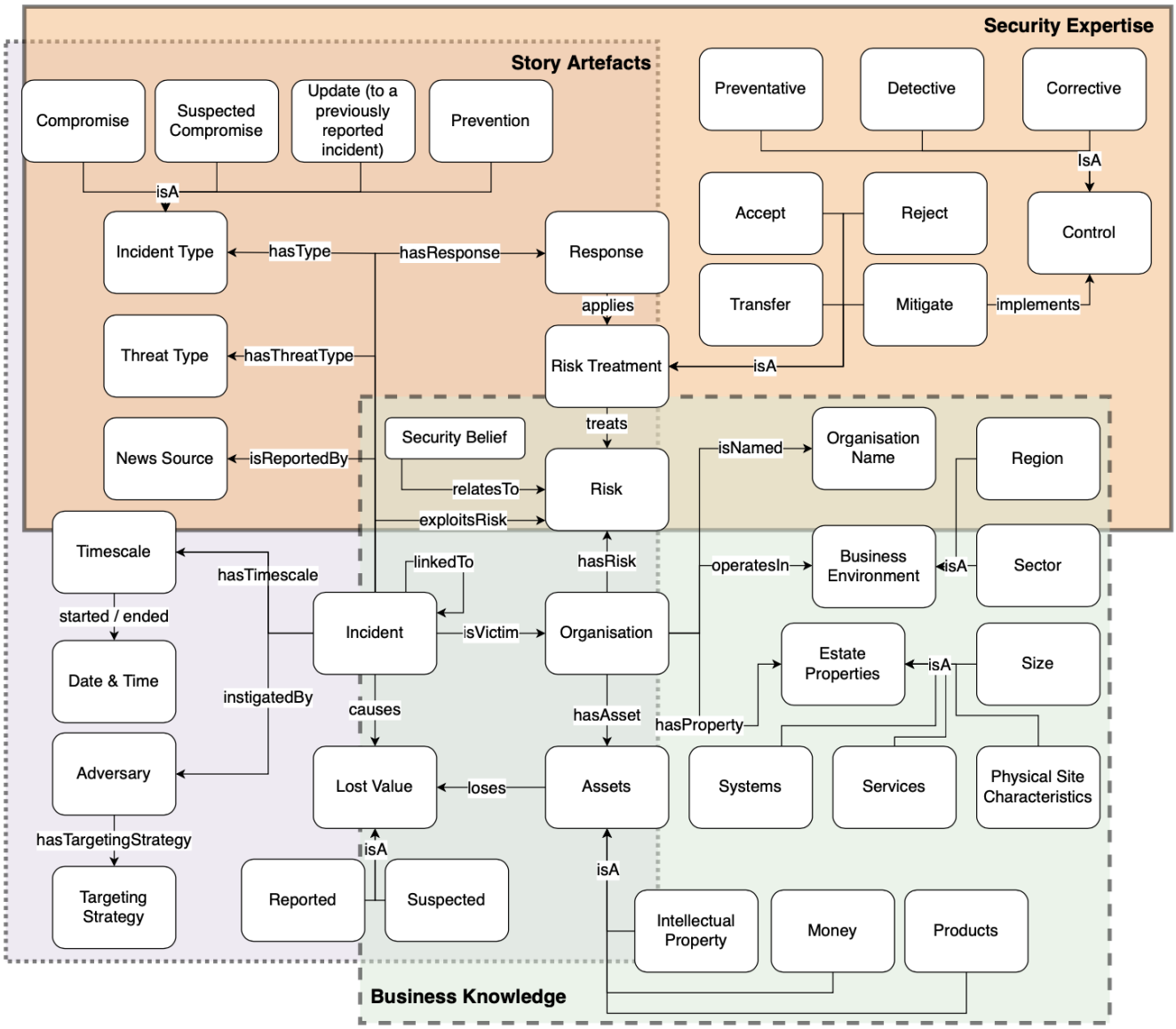

Figure 3: Ontology design, with *indicative* demarcation of domains of information relating to Business Knowledge, Security Expertise, and Story Artefacts. A conversation would be prompted by details of the incident at the centre of a story, with potential to connect to information that the business leader or security advisor is more familiar with from their own domain.

[14], security stories [44], and information sources for informal learning [43].

- Incident / Story (inc. news source)
  - Incident Type [compromise | suspected compromise | update (to a previous reported Incident) | prevention)
  - Company Name
  - Business Environment Descriptors
    - Region (Country and Region / City)
    - Business Sector
- Business Activity Descriptors
- Threat / Attack Type (can be multiple)
  - Mechanism of Threat (can include specific combinations of Business Estate Descriptors, Business Environment Descriptors, and/or Business Activity Descriptors)
  - Target of Threat / Attack (can be multiple)
- Business Estate Descriptors (can be multiple in each subcategory)
  - Size (can be measured as specific Income/Turnover, informal Size descriptor [Micro | Small | Medium | Large], no. of employees | volunteers | members)
  - Systems
    - Link to Physical Computing Asset instances

  - Services
    - Link to Digital Service Asset instances
  - Physical Site Characteristics (acknowledging mixed-mode Threat / Attack Types)
- Assets
  - Can link to any of Business Descriptors
  - Money | Intellectual Property | Products | Data
- Loss [Reported | Suspected] - link to Asset type or instance (depending on if Incident is speculated or confirmed)
- Technical Resolution (actual - part of story | suggestion - advice that was inserted into the article) (this can include prevention of an incident) (can be multiple)
- Linked Incident / Story (can be multiple - may be reported elsewhere, potentially with different details, especially where there is speculation as to what occurred)
- Risk Treatment approaches (comparable to, e.g., [14]).

It is important also to include timestamps of information, especially in evolving stories/situations, where an ontology encoding can allow this to be captured alongside ontology elements. It is important for situational awareness to be able to support management of security while working with imperfect and fragmented information. We also signpost the Security Belief around a news story, as in Figure 3, where there is a distinction between Security Thinking and Security Behaviour [44]. Changes in thinking – and beliefs – around security precede change in Behaviour (or in this case, arrangement of a decision-making process as to whether to change the security of an organisation).

3.4 Example ontology instance – ransomware

Here we refer to an article from BBC News, "The ransomware surge ruining lives" [55] ('News Source', as in Figure 3). This story describes a number of related ransomware attacks. These represent instances of actual 'Compromise', by a defined 'Incident Type' (ransomware).

3.4.1 Business knowledge. Some way into the article, there is description of an attack on a company with 230 employees. The company is named ('Organisation Name'), but their sector is not mentioned, so there is 'Size' information, but also that they are a Swiss company, providing 'Region'. The story mentions that the company has a website ('Systems').

3.4.2 Incident knowledge / story artefacts. It is mentioned that the company website was affected (image assets on the website were encrypted), and that the incident occurred in May 2019 ('Date & Time'). 'Lost Value' is implied by the mention of there being 'tens of thousands' of pending orders. A 'Timescale' could be implied by the mention from the company's chief executive of the incident being "the worst three weeks of my life".

3.4.3 Security/threat knowledge. The 'Adversary' was named as the Ryuk gang. A 'Security Belief' of note here was that the cost of rebuilding the business was approximately the same in cost as the ransom that was demanded (45 Bitcoins, or at the time 'half a million dollars', adding to the 'Lost Value'). A 'Response' option was then highlighted, of not considering to pay the ransom but to instead use the equivalent amount to rebuild the digital assets or 'Systems' of the business.

3.4.4 Partial information. As can be appreciated from the description above, this article can be used to populate at least a partial instance of the ontology. The ontology can then be used as a prompt for the leader of an organisation, whose context relates to the information in the story, to start a conversation with an IT advisor. What is also of note regarding the example news article is that it includes commentary from at least two companies providing cybersecurity expertise, including that "66% of victims admitted to paying part or all of the ransom" (hinting at a 'Risk Treatment', but notably without mentioning particular kinds of organisation).

Regarding the 'Targeting Strategy', the article only mentions that "Hackers use malicious software to scramble and steal an organisation's computer data", but not how they gain access to that data; an IT advisor may be able to walk through a business leader's IT systems to identify vectors for an attack (if there are any). There is then not enough information in the article to inform whether the 'Hackers' (as 'Adversary') are a threat to a particular business, to then be able to navigate 'Security Beliefs' relating to their organisation. Also 'computer data' as a targeted 'Asset' is both applicable to most businesses but also general, where this would impact how a business leader *prioritises* a security-related decision relative to other decisions they have to make. An ontology may better inform a richer conversation about investment decisions, but conversations are not deterministic. They will not definitely lead to the best decision emerging from discussing an incident.

3.5 Navigating stories together

The ontology tool would allow for details of a news story or anecdote to be given a formalised structure, in turn supporting use by business and security people exploring solutions together (Section 3.1). News stories and anecdotes may be 'complete' in themselves, but not as full security descriptions, owing to limitations in the format or available facts. They are not an instruction manual or tailored guide for either a business leader or IT specialist. Neither are they about the specific business or security context of the business leader's own organisation, but there may be *similarities* and *differences*. However, this is a starting point distinct from one-way interventions which may impose advice but not inform the *why* and *when* of how that advice matches to the business.

A 'better' story is then arguably one which can *be linked* by each side of the conversation to other resources, knowledge, guidelines, or indeed other news stories that one person or the other in the conversation is familiar with. For instance, a news story or anecdote may refer to a widely-used operating system or service used by many companies, such as Blackbaud [25] or Kycera [4]. A connection could then be made to procured IT – *"does this business use this service?"*, *"can similar services or systems be attacked in the same way, and are our IT assets similar?"*. If specific business properties are mentioned in a news story , such as a specific sector, this serves as a reference point from the business perspective, which can be followed into the ontology to explore other similarities.

We also do not want to alienate the security specialist in this shift. As shown in our Background section, however, existing knowledge-sharing initiatives are aimed at – or presume – existing security expertise, even while purporting to support businesses. If a specific attack vector, vulnerability, or malicious tool is mentioned as

having been used to compromise a business (such as a particular ransomware kit), this leads into specialist security knowledge. The *relations* between ontology concepts mean that these connections can be followed from the perspective of either side (Section 3.1).

If there is less detail in the anecdote or news story brought into the conversation, an ontology may be used to bring in comparable news stories for discussion, linked to through the connections between ontology elements. This enriches the conversation with further concrete details to compare and contrast, without requiring news stories or anecdotes themselves to become 'better' resources. If that were to happen, it would stray into the realm of specialist IT/security news, and away from opportunistic sharing of information between business leaders and their peers.

A less useful form of news story would be one where the security element is still highly speculative, relying on conjecture to establish how it relates to a business. This might be the case in ongoing stories of active IT system compromise, or complex stories where the circumstances leading to a security incident are as yet unclear. In such cases, 'repeat conversations' may happen around a story, to 'watch' ontology content develop.

3.6 Respectful use of stories and anecdotes

To inform investment decisions (Section 3.1), we must address how an ontology would support a conversation started by a story, or by an anecdote. A conversation cannot happen without an initial point of common understanding, so key to any use of the ontology would be to find some details to start from. We also should respect the authenticity present when an anecdote is shared, as it is often received from peers who mutually trust each other. In this sense, knowledge support can have a use in substantiating anecdotes (or indeed news stories from sources which have not been corroborated to the reader's satisfaction), gradually linking understanding to the partial details brought to the conversation.

The concept of trading zones [18], has been proposed as a means to bridge between scientific as well as security communities [54]. This has relevance also to conversations between business users and IT advisors. The fundamental concept is not to impose one language or terminology over another when communities interact or share knowledge. Instead, the proposal is to identify a common language shared by all sides of the conversation, which will facilitate meaningful dialogue in a particular context. Here we apply this approach around the evidencing of security investment decisions, a trading zone between knowledgeable parties who may be applying evidence-based reasoning much as scientists would. Galison notes that *incomplete coordination* may occur, using partially interpreted objects with a fundamental property of being *exchangeable*. We regard anecdotes and news 'headlines' as exchangeable artefacts in a conversation.

We further consider the ontology tool described here as facilitating this exchange, with elements of news stories serving as 'regularised' artefacts with which each side associates their own meaning, but which both sides recognise and can parse relative to their own professional background. Use of an ontology tool within this context of knowledge exchange facilitates the *coordination* which Galison refers to as important in these trading zones. The ontology steps in to facilitate a mix of boundary objects and interactional expertise in security management [9]. Where there are exchangeable artefacts, such as elements of a news story, we expect that these can be understood in their own ways by each side of the conversation; the greater the number of artefacts and accompanying details which can be regularised by each side, the more prolonged and meaningful the conversation can be.

Calibration of the different views represented in the conversation may come from first discussing the 'Incident' and associated 'Security Beliefs', as in Figure 3. The news story or anecdote itself could of course be discussed as a foundational artefact, to identify which elements of it may be perceived as relevant information which can be exchanged. This would establish a shared understanding, in the conversation, of 'what happened' in the news story or anecdote. Elements such as the 'Compromise' or 'Targeting Strategy' may feature, when the incident relates to the business leader's organisation, as part of the "could this also happen to us?" conversation.

Either side may question the links that the other person makes from the story/anecdote elements back to their own area of expertise. This can include examining not only 'Security Beliefs' but also narratives about the business which relate to those beliefs [49], and other factors which can contribute to resistance to what would otherwise seem like reasonable proposals for change [17]. Disputes as to any suggestions for investment may relate instead to imperatives outside of the context of the security incident in a particular story or anecdote. This could include issues such as business continuity over the disruption of introducing new IT solutions or decommissioning older systems. Another example would be disputes around the timeline of an effective change (relating to 'Timescale'), and when an investment needs to happen – these potentially become more a case of informing the business leader and allowing them to make an informed choice.

4 POSITIONING AND DELIVERY

Forms of *informal learning* about security from stories and anecdotes is haphazard [43], and the emergence of those prompts then up to chance. In this section we explore approaches to position the tool described in Section 3, but also who could broker access and facilitate the security conversation. Referring again to tenets of community transformation [5], the role of engagement is recognised alongside that of good design, including the spaces where change is facilitated.

4.1 Positioning

One-way advice has its merits if delivered in ways that make it useful for recipients [45]. However, expert-led interventions address *"community-as-problems-to-be-solved"*, with a focus on implementation and tangible results [5]. For businesses, advice interventions most likely rely on proactive effort from business leaders to go beyond their area of expertise and normal channels of information. We position our proposed approach as standing separate from these platforms of expertise, including many discussed in Section 2 such as advice web-pages, targeted adverts, prompts from IT hardware itself, and signaling from regulatory mandates. Some channels, such as community events attended by trusted peers, may also help to relate a business's existing antenarratives – beliefs and stories about a business, and businesses like it – to a news story [49].

To consider instead supporting the conversation about security, the ontology is useful in a range of contexts where security choices could be explored (rather than dictated), including the following:

4.1.1 Addressing sporadic concerns about security. There may be regular or irregular interaction between a business leader and their trusted IT/security advisor. In some cases this may be a one-way request to the advisor to simply 'sort out this thing I read about'. Generally speaking, these interactions could be a learning opportunity where the security specialist will respond to clarify whether a story is relevant or not. This highlights another blending of individual and organisational dynamics, between a formal IT/security support contract and an individual seeking 'informal' technical support [42]; the person providing support may defer helping, solve without explanation, provide limited help, or provide in-depth help. Regarding learning opportunities, the support person may also leave the other party repeatable instructions or provide an explanation of their proposed actions. The latter may qualify or dampen business leaders' concerns when they next read a comparable story about organisation security.

4.1.2 Qualifying security needs. A *conversation bootstrapping tool* between an IT provider and their customer base, to explore options for security investment across a subset of comparable businesses. A support person may choose to provide unsolicited advice [42] *before* being prompted by a business leader, where in this case the utilisation of the ontology tool would likely be led from the security side, rather than individual businesses. This is an opportunity to empower the IT provider [48], who can have related stories available when reviewing security provisions for clients, based on their existing knowledge of what customers already have in place. If there are anecdotes to substantiate, e.g., *"I've heard that password managers aren't always reliable"*, the underlying beliefs can be explored. Similarly, an IT provider can have stories available for business leaders to 'compare' themselves to, or broadcast potentially relevant stories to clients to probe whether they are relatable; this approach respectfully accepts that the advisor may not know everything that there is to know about the business. If the outcome is a selection of advice or controls based on business characteristics, this becomes akin to *personalised nudging* [32].

4.1.3 A foundation for the socialising of security. A resource for peer community events, as opposed to strictly security-themed events. 'Communities of practice' have potential for improving cybersecurity approaches in smaller businesses [36]. Stories – or case studies (Section 4.4) – could be an icebreaker to encourage conversations about security, around which a number of business leaders can discuss their differences and similarities. Where groups of peers relate to particular details, the social influence of security has the potential to encourage change [11]. Closed events between trusted peers, including those following 'Chatham House' rules of discretion [11]), would likely include stories and anecdotes already. Having structured details available, extracted from news articles or anecdotes, can support a more detailed discussion in that moment. This would be rather than conversations which remain unsubstantiated and risk not producing facts which inform any subsequent business decision-making, as interesting and engaging as they may otherwise be.

4.1.4 Local community alerts. Interventions can increase their reach to smaller businesses by engaging at a local community level [48]. Within the scope of supporting community-driven transformation, entities such as regional government or police forces may facilitate engagement with security stories and conversations around them. In the case of security alerts or advisories of emerging threats, this could be further driven by focusing on where prompts are occurring in the local community and positioning support there, as opposed to broadcasting advice from one central advice point. Similar to the previous scenario, these local authorities are naturally in a position to arrange events which are not *directly* about security, but where the topic may come up in conversation with business leaders opportunistically. Positioning of the ontology in this case is about being ready for a dialogue, as opposed to having an agenda that demands that security be discussed.

4.1.5 Augmentation of existing regulatory subscriptions. The problem of building a tool may be tractable, but a far greater problem exists for increasing awareness of such tools to those who could benefit but who would otherwise not be aware. Organisations may be registered to an existing reporting and governance relationship with authorities, e.g., data protection regulations or sector-specific regulations and reporting, as for charities in the UK. The dissemination of stories can then be an enabler of a nation's data protection strategy, or similar. Key here is leveraging a pre-existing 'non-security' touch-point. In some states that legislate for the European Union's General Data Protection Regulation (GDPR), organisations that handle personal information must pay an annual data protection fee to the office of their information commissioner. Where any such processes record information regarding organisational properties (as in our ontology), this could be used to provide notifications of news stories which are relevant.

4.2 Facilitating access and engagement

To one extent or another, the avenues for positioning the ontology tool, as above, are already happening , and we are exploring respectful ways to have security knowledge ready to support those particular conversations. This would be in the spirit of community-driven transformation where businesses are already leading their own development – the security community must identify appropriate ways to support this, rather than assuming to dictate the change, as with typical advice interventions.

Data may be gathered from news stories. This relies on outlets ideally being readily accessible (i.e., not behind paywalls), and trustworthy (specifically, that the reporting is factually correct). Incidents which are not 'entertaining' may not make it to a news publisher, let alone to a prominent place in a business leader's favoured news source. This speaks again to the role of positioning to make the most of available stories – business leaders cannot be assumed to know about all stories and anecdotes relevant to them.

To systematise the capture, compilation and dissemination of stories, we would propose the use of the ontology with a graph database. Data of subscribers would need to be captured in addition to the information pertaining to the stories. The collection of such

[11] https://en.wikipedia.org/wiki/Chatham_House_Rule

data allows for the matching of subscribers to related stories, either as new stories are added to the knowledge graph or as a scheduled event, depending on the use context as in the previous subsection. Automated means could then help to 'prepare' an ontology from anew or as derived from a larger dataset, to meet the business context of event attendees.

Prompts produced by varying levels of automation could also be possible. A recommendation algorithm could traverse the graph to pair subscribers with news stories. Notifications could be transmitted through the subscriber's accepted means, such as email, instant messaging, RSS, etc. Communal discussion of ontology content could also be facilitated by a trusted security specialist, or in ad-hoc conversations with peers, for instance to ask targeted questions to qualify how security relates to particular aspects of the digital estate, such as the presence of outsourced IT, social media capabilities, or a managed supply chain. This acknowledges that comparable businesses could have gone through related experiences, but be unaware of each other, as is an aspect of the haphazard nature of informal learning [43].

As highlighted in our discussion of potential options for positioning the ontology tool, the place where information is presented is key too. Positioning information on a website makes it accessible, but assumes that businesses know about it or regularly check for new information. This is not sufficient, especially if new security threats emerge regularly. Ideally, it would become part of what businesses already do, and the channels they already use. Rader et al. [44] note also that the *context* around a story is important and can influence whether a story changes behaviour. This includes who is conveying the story and where, such that a casual context can strengthen behaviour change, and stories delivered by seemingly more knowledgeable people can also positively influence outcomes.

Most news stories refer to incidents such as data breaches. Ideally where there are more 'positive' stories, these could be included in the ontology as well, as further learning opportunities. What is of great value about positive stories is that they are more likely to be framed around what may have been done to avoid or recover from a negative outcome. This would not necessarily be the same as exploring 'near misses', where negative outcomes were narrowly avoided – such a discussion would test the causal understanding of how security incidents unfold, and may lead to conjecture which undermines the trading zone between both sides. In terms of stories remaining both pertinent and entertaining, it seems viable for stories of businesses 'heroically' avoiding an incident or which have a positive ending to still be a captivating read.

Where we have identified constructive approaches in Section 4.1, non-constructive approaches would be those which encourage (especially smaller) businesses to attain a fixed, recognised standard of security protections and controls, ignoring the particular details of an individual business. Implicit in the vehicles for support described in Section 4.1 is that the stakeholders managing use of the ontology have a need to, or only realise benefit by, providing effective advice and by respecting the needs of the business. This requires some understanding of business needs, rather than focusing on security above all other imperatives.

Other forms of news articles or anecdotes which may not make for constructive content in the ontology could be those incidents where there were disastrous or large-scale consequences, i.e., not just that the story does not fit the business of the reader, but also that the efforts needed to address such an attack would be beyond most organisations. An example of this would be a story involving a targeted, highly-resourced attacker, typically attacking a large organisation, as can often be headline news.

4.3 Supporting divergent audiences

Small-to-medium businesses are known to be diverse in their IT and IT-security needs [40]. Population of an ontology instance may be associated with relationships between business leaders and IT advisors. Referring to the different forms of engagement listed in Section 4.1, there may be one or more business leaders on one side, and an IT advisor of varying affiliation on the other (be it an IT provider company, business association advisor, etc.). We presume the IT advisor maintains and curates an ontology instance, for a group of businesses with similar traits, or potentially for individual organisations if their needs are especially complex. Use of the ontology may then scale, with one instance being useful for many businesses, albeit for their own distinct conversations.

Businesses of varying sizes and sectors may differ in their perception of risk, implementation of security controls, and experience of security incidents [22]. These differences may be moderated by sector if a business association is managing the interaction, or require divergent instances of ontologies populated by one advisor where, for instance, an IT services provider has a a range of clients of varying size and sector. The 'Business Environment', 'Estate Properties' and 'Assets' properties of an ontology (Figure 3) can be analysed to navigate ontology instances and link stories to multiple instances. If different businesses use varying terminology, this may be reflected in the 'Business Environment' and 'Estate Properties'. If so, these properties may require focused discussion to unpack them as part of the conversation.

Future research may explore the capacity to record the 'history' of particular kinds of companies sharing certain business properties (so that in effect, many organisations can learn from each others' experiences). We note here that often security interventions presume no 'memory' of what companies have already done to secure their businesses, whereas the ontology could be used to navigate and 'tick off' what is and is not already in place in an organisation.

We expect that anecdotes would provide fewer, or less specific, details for use in the ontology, but these can still be useful for recording recurring concerns. For example, the BBC News story mentions 'Hackers', something of a general term which does not indicate much regarding the intentions or capabilities of the malicious party. Anecdotes may contain information framed in a similar way. This is where a conversation with an IT specialist, by way of concrete knowledge, would explore the 'Security Beliefs' of a business leader, and whether they arrive at a conclusion that they believe the 'Hackers' mentioned in the story might target their business. This may be determined by comparison with details from a news story, for instance where the size of a business is mentioned, *"is our business at a similar risk if it is the same size as this business which was compromised?"*. This again challenges security beliefs, in this case that such an attack could genuinely happen 'to a business like ours'. That a business leader brings a story or anecdote to an IT specialist already signals that they think it is plausible; if stories

refer to differentiating factors such as business sector, this further allows a business leader to decide if the threat *needs to be acted upon* as an investment decision. This again links to the stories and narratives particular to individual businesses. Not all comparable businesses are managed in the same way, which already influences attitudes to 'Risk Treatment' and how business leaders believe they can protect their 'Assets'.

4.4 Case studies and navigating the ontology

Resituating knowledge from its original context to another is not straightforward [34]. General-level advice is disassociated from a specific 'local' context; our proposal assumes that a business leader would be guided somewhat by an IT advisor in exploring whether knowledge can be translated from the original context of a story or anecdote to their own, one case to another.

There are different strategies to resituating knowledge [34], where the ontology content would be used most readily as a 'bridge' from the specifics of one case to another, in situations where there are direct similarities. These could be the same similarities that prompted a business leader to believe they needed to take action. News stories and anecdotes are analogous to 'messy' and incomplete case studies; the construction of their content is according to some mix of completeness sufficient to convey the story, and it being an interesting story. Anecdotes are yet more minimal in detail. An implication here is that not all news stories will have enough knowledge to be resituated, but nonetheless can prompt the conversation about security.

Links to other cases through ontology relations then have further benefits. This would require there to be 'ladders', to facilitate desituating knowledge from the context of one story to a general level, and exploring whether it can be resituated down to the business leader's local context, or otherwise compared to another story. This is in essence what we saw in the example in Section 3.4, reports of specific cases of ransomware attacks, loosely related to general advice – 'stepping stones', bridges, or ladders are necessary to relate a case to a different business.

The IT advisor would more readily facilitate the 'ladder' approach and how to determine if knowledge can be resituated. The relevant properties of a business in a news story could be inferred, as part of the shared dialogue between business and security. For example, a story may mention a popular software product which is part of a suite of applications often packaged together and used by many businesses, such as Microsoft, SAP, etc. This relies somewhat on being able to make connections, which is a goal of the ontology. Advice which 'misses the mark' lacks those connections.

Inferring and exploring the relations between pieces of ontology content is akin to exploring the mechanisms [53] which underpin a threat or which would encourage a specific investment, as the event which prompted engagement. For the latter, this would be a security control or change which can be enacted in the shared belief that it would address the threat. As IT-security systems are engineered mechanisms [20], an IT advisor may suggest an investment which *they* believe addresses a concern. Engineered mechanisms can be influenced by attackers, but also undermined by not being the right investment to address the threat.

In security generally there is a lack of discussion of what has gone right, where exemplar case studies are often those which are at the extremes [34] (e.g., large-scale and rare cybersecurity incidents, or idealised descriptions of complete and comprehensive, aspirational security infrastructures). The latter are at risk of being exploited through Fear, Uncertainty, and Doubt (FUD) [23], to encourage investments where they are not needed. Sensational news stories would feed such narratives. FUD essentially obscures the 'stepping stones' and connection between a business's context and the proposed investment, leveraging risk aversion over the feasibility of a solution. This relates to the proposal for *concordance* in security [1], and the importance of agreeing not only on a shared goal of securing a business but also on feasible ways to get there. Doubt can have benefits in generating possibilities during sensemaking activities [28], and can be part of changing mindsets and expectations.

4.4.1 Moving from ontology content to static case studies. Maintaining an ontology instance for each communication vehicle (Section 4.1) may be a cumbersome approach, in terms of maintenance and immediacy of access. It may be possible instead to generate 'constructed' case studies which resituate knowledge from a series of cases to then present a 'typical' case [34].

Given the diversity of smaller businesses, it may be necessary to have an established range of 'typical' IT configurations [40] with which to associate cases. A case study aimed at all 'small businesses' likely will not address a 'typical' environment across all of them, and so will lack any 'bridge' from the case study to the local properties that a business leader can recognise in their own business. 'Exemplar representatives' may be possible for very rigid IT systems, such as off-the-shelf productivity applications, or where a news story may include something of the nature of 'this threat affects all versions of this operating system'. Certainly, an issue with one-way general advice to businesses is that in its generality it presumes to apply to some unspoken 'constructed representative' case [34]. Providers of advice could well benefit by declaring the assumptions or exemplar case they have in mind when constructing what they presume to be broadly-applicable advice.

In terms of tooling, a differentiation between ontologies and alternative and less resource-intensive tools would link to this also. Put simply, case studies would be a 'static' distillation of a discussion that would otherwise use the ontology and its moving/dynamic parts. Case studies could then be a 'flat' output of an ontology instance.

5 DISCUSSION

Here we have proposed a new approach for how security advisors can engage with businesses. Consideration must also be given to assessing how the paradigm achieves its goals over time. Typical interventions, such as advice web-pages, may be measured by the number of page views. Measures of exposure to an intervention do not necessarily indicate actual enactment of the advice. In the case of the transformation activities we propose to support, transformation may not be measurable within the timeframe of any one particular 'campaign' (as would normally be the case with a particular intervention), but instead could take a long time, if it happens at all (which would not be guaranteed). With this in

mind, a similar approach to that described for within-organisation 'security dialogues' [1] could be adopted; this involves measuring not the outcome of the interactions between domains of expertise, but the qualities of the interactions themselves. This could include, for example, how often businesses have a discussion with their IT/security advisor, or whether particular security options were considered but not adopted due to resource limitations. For instance, there is in essence no data to indicate how many companies have considered adoption of particular security guidelines, but chosen not to do so because of some prohibitive factor such as cost.

Understanding the qualities of the security conversation can inform interventions *around* the conversation. That is not to refer to opportunities to sway the conversation itself, but to instead ensure that options are available to cater to as many concerns as possible – this is to acknowledge that (especially smaller) businesses are not always in a position to have security solutions crafted to match their particular organisation circumstances. For example, they may have bespoke solutions which are in reality separate productivity applications securely knitted together; very small businesses may be using software more like that of the individual user. It is then complementary to the security conversation to have solutions available as possible 'answers' to anticipate 'questions' about how to address a concern (as raised in a news story). Relating to behaviour change [16], this is akin to ensuring there are desirable solutions which match to the Ability and Motivation available within any business, such as basic or default security protections available for any budget. It can also be that business leaders perceive a cybersecurity solution as affordable, but that whether they can be maintained to ensure secure working indicates a need for more adequate solutions to be engineered [38]. This relates to the historic mission of security solutions and support to cater primarily for the needs of critical infrastructure and governments [15], potentially requiring more localised creation of security solutions to match comparable sets of businesses [40]. There may be resistance to change [17], especially if a business leader believes they do not have the resources to invest in security [38], so identifying accessible and minimally-disruptive solutions is beneficial.

5.1 Management of a respectful tool

The notion of community may emerge to moderate bad or FUD-driven [23] security approaches from entering the ontology, and to maintain *relations* to good practices. Good practices would be maintained in two ways, requiring engagement from other stakeholders. Higher-level or business-agnostic advisory groups may act in the interests of businesses to not so much help them arrive at a specific 'Response' (Figure 3), but to assess the available 'Response' options. A second way to moderate the ontology is in business leaders continuing to talk to peers and share anecdotes – the ontology does not replace this, but instead augments it. If their experiences indicate that an existing approach was effective, or a new approach not effective, they may share these experiences with each other, prompting a review of the ontology content with an IT advisor.

In this way, although it would be necessary to set up and actively use the ontology tool, it could in time serve as a 'memory' of the concerns and conversations involving particular organisations. This could offset the need to integrate the ontology into practice as an additional tool, acting almost as an ongoing measure of organisations' beliefs and needs. As implied in the various forms of conversation in Section 4.1, there would need to be two parties involved in the conversation of navigating the ontology and any stories it contains. Populating an ontology instance only to instruct businesses to peruse it unassisted not only breaks the idea of a conversation, but also of two-way expertise, while also adding additional burden to business leaders to become experts in security.

Alternatively, in measuring the quality of interactions, the nature of the questions and concerns that a business leader brings to the conversation could indicate something of the security maturity of the business. Such a 'memory' of interactions could complement delivery approaches as described in Section 4.1 as they repeat over time, mapping the capacity of leadership to query the security of their own business to parts of the ontology.

Skills are then necessary to be able to guide a business leader in exploring the needs of their own business. A humble approach may be necessary, where listening and enquiry are as important to the advisor as providing advice [51]. A similarly humble approach to ontology maintenance would be to point to other ontologies rather than reproducing content or presuming to manage it centrally, where this points to detection and subscription approaches as in Section 4.2. This distribution of maintenance can also be useful for signalling whether knowledge is still relevant and correct for businesses.

5.2 Limitations in the scope of the paradigm

Our proposal to leverage security stories for business decisions is limited in terms of the capacity to prepare businesses for 'anticipated' problems, which have not happened to any business yet, and hence have no reported instances. There is already a lot of advice to businesses that focuses on *preparation for potential threats*, though as we have discussed in the Background section, such advice is limited in its potential to resonate with businesses. Approaches may then default to regret-based behaviour change and fear appeals, either to businesses [23] or individuals [47]. These will have a marginal effect if they do not also come with information to empower the recipient to address the cause of concerns [21, 47], here being whether particular business-related decisions have to be made. The approach relies on a presumption that there is someone to tell the story of an incident – where there would be less visibility is regarding stories about organisations which suffered existential incidents. In these cases, there is nobody remaining to tell the story afterwards, such as if an organisation is wound down as a consequence of the (e.g., financial) impacts of the event.

There is also a need beyond the immediate uses of the ontology, and the security conversation, to consider safeguards against taking the *wrong action*, especially after discussing a potentially inaccurate story. We presume that in most cases the conversation about security would qualify the appropriate course of action, this being a key motivation for proposing the ontology. This highlights that our proposal appropriates an existing medium (news stories) for something other than, and as well as, its primary purpose, as opposed to information sources dedicated to clarifying more technical

details, such as technical forums [43]. This points to the potential for knowledge exchange that amounts to 'misinformation' [8], requiring care in the *curation* of ontology content to produce objective evidence. However, there may also be narratives which evolve over long periods of time which are difficult to prove as inaccurate, for instance in the reporting of suggestions that computer chips had 'backdoors' engineered into them at manufacture[12], which impacted infrastructure and investment decisions at a large scale.

6 RELATED WORK

The 'Security Dialogues' research [1] explored the interaction (or lack of) between IT/security staff and employees within organisations, through a series of interviews and subsequent workshops which brought both sides together – a goal in the work was to support more positive dialogues between the two domains of practice. Trust between both sides emerged as a critical factor, as did a perceived lack of consideration for the imperatives of either side. The workshops involved sessions focused on how to ask questions (and allowing participants to act on this), to probe the differences between the perspectives of participants from both sides of the relationship. Where the authors pursue tools for policy *concordance* – agreement between both sides on appropriate solutions – our work, within the dialogue between business leaders and security specialists, also considers approaches to support the prompts for that engagement to occur.

Njenga and Jordaan [35] conducted qualitative research with smaller businesses, to examine neutralisation – or rationalisation – approaches to specific security measures such as maintaining data backups. Instances were found where the ways of working within a business would clash with advocated best practices for security (such as allowing all employees to have access to the entirety of company data, on account of it being comparatively small business). Where the authors focused on the gulf between these neutralisation approaches and advocated practice from the security side, we consider that such approaches may emerge from business leaders' decision-making process about how to fit IT to the business – practices emerge when security is rationalised alongside other business imperatives.

Lewis & Coles-Kemp [26] explore the potential for visual comics as a vehicle for building narrative scenarios to represent security-related tasks. Personas were constructed to represent the tasks and concerns of information security practitioners, in the accessible format of a comic. In our work we explore the underpinning information, and leverage a news story as the central object of discussion – it may be that a visual comic is another viable format, where Lewis & Coles-Kemp similarly acted to capture enough details to prompt engagement and discussion of factors in security-related concerns. Considering other visual forms of engagement Hall et al. [19] explored the potential for Lego blocks to be used by a group of employees from across different parts of the same organisation to reach a common understanding of the IT and security-related components of their work, pointing to further forms of engagement which can be considered when both business leaders and security specialists enter into a dialogue about a pertinent security concern.

[12]https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies and https://www.bloomberg.com/features/2021-supermicro/

7 CONCLUSION

We have explored the opportunities created by recognising the conversation between business leaders and security specialists as a 'trading zone'. We have explored how supporting the trading zone can be a route to sustainable, workable security improvements. We see also that effective prompts for change are already present, as the stories that reach business leaders through news sources, or as anecdotes from trusted peers.

We have demonstrated this shift in perspective by recasting a decision support tool which favoured security expertise – security knowledge ontologies – to support different perspectives in a conversation about security. By framing our proposal within a broader view of community transformation, we further explored how transformation support can be resourced and positioned alongside typical 'intervention' options such as advice web-pages.

Future work will engage with leaders of smaller businesses and ideally their trusted security advisor, to study the security conversation itself and the actions of both parties following their interaction. Engaging with business leaders directly will allow us to explore what makes a story compelling for them, but also effective for their IT advisor as a means to navigate the business leader through a range of cybersecurity investment options. This can lead to exploration of other existing security tools which can be recast as more respectful of business expertise, where here we have focused on ontologies and also explored case studies.

ACKNOWLEDGMENTS

The authors wish to thank the paper's pre- and post-event NSPW shepherds – Jassim Happa and Karen Renaud, respectively – and the original reviewers of this paper for their insights and guidance. We also wish to thank our session scribes and the attendees of NSPW 2021 for their detailed feedback on this work.

REFERENCES

[1] Debi Ashenden and Darren Lawrence. 2016. Security dialogues: Building better relationships between security and business. *IEEE Security & Privacy* 14, 3 (2016), 82–87.
[2] Maria Bada and Jason RC Nurse. 2019. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security* (2019).
[3] Yves Barlette, Katherine Gundolf, and Annabelle Jaouen. 2017. CEOs' information security behavior in SMEs: Does ownership matter? *Systemes d'information management* 22, 3 (2017), 7–45.
[4] BBC News. 2021. Ransomware key to unlock customer data from REvil attack. https://www.bbc.com/news/technology-57946117
[5] Peter Block. 2018. *Community: The structure of belonging.* Berrett-Koehler Publishers.
[6] P. Briggs, D. Jeske, and L. Coventry. 2017. Chapter 6 - Behavior Change Interventions for Cybersecurity. In *Behavior Change Research and Theory*, Linda Little, Elizabeth Sillence, and Adam Joinson (Eds.). Academic Press, San Diego, 115–136. https://doi.org/10.1016/B978-0-12-802690-8.00004-9
[7] Madeline Carr and Leonie Maria Tanczer. 2018. UK cybersecurity industrial policy: An analysis of drivers, market failures and interventions. *Journal of Cyber Policy* 3, 3 (2018), 430–444.
[8] Tristan Caulfield, Jonathan M Spring, and M Angela Sasse. 2019. Why Jenny can't figure out which of these messages is a covert information operation. In *Proceedings of the New Security Paradigms Workshop*. ACM, 118–128.
[9] Harry Collins, Robert Evans, and Mike Gorman. 2007. Trading zones and interactional expertise. *Studies in History and Philosophy of Science Part A* 38, 4 (2007), 657–666.

[10] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A typology of perceived triggers for end-user security and privacy behaviors. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX.

[11] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX, 143–157.

[12] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 1–12.

[13] Department of Digital, Culture, Media and Sport (DCMS) (UK). 2021. Cyber Security Breaches Survey 2021. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021

[14] Stefan Fenz and Andreas Ekelhart. 2009. Formalizing information security knowledge. In *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*. ACM, 183–194.

[15] Ivan Flechais. 2015. Towards a Model of Information Healthcare for Household Data Security. *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)–Poster Session* (2015).

[16] Brian J Fogg. 2019. *Tiny habits: The small changes that change everything*. Eamon Dolan Books.

[17] Jeffrey D Ford, Laurie W Ford, and Angelo D'Amelio. 2008. Resistance to change: The rest of the story. *Academy of management Review* 33, 2 (2008), 362–377.

[18] Peter Galison. 2010. Trading with the enemy. *Trading zones and interactional expertise: Creating new kinds of collaboration* (2010), 25–52.

[19] Peter Hall, Claude Heath, Lizzie Coles-Kemp, and Axel Tanner. 2015. Examining the contribution of critical visualisation to information security. In *Proceedings of the 2015 New Security Paradigms Workshop (NSPW)*. ACM, 59–72.

[20] Eric Hatleback and Jonathan M Spring. 2014. Exploring a mechanistic approach to experimentation in computing. *Philosophy & Technology* 27, 3 (2014), 441–459.

[21] Cormac Herley. 2013. More is not the answer. *IEEE Security & Privacy* 12, 1 (2013), 14–19.

[22] Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Dominik Wermke, Yasemin Acar, Arne Dreißigacker, and Sascha Fahl. 2021. A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In *30th USENIX Security Symposium (USENIX Security '21)*. USENIX Association.

[23] Andrew Jaquith. 2007. *Security metrics: replacing fear, uncertainty, and doubt*. Pearson Education.

[24] Paul Jones, Geoff Simmons, Gary Packham, Paul Beynon-Davies, and David Pickernell. 2014. An exploration of the attitudes and strategic responses of sole-proprietor micro-enterprises in adopting information and communication technology. *International Small Business Journal* 32, 3 (2014), 285–306.

[25] Leo Kelion. 2020. Blackbaud: Bank details and passwords at risk in giant charities hack. https://www.bbc.com/news/technology-54370568

[26] Makayla M Lewis and Lizzie Coles-Kemp. 2014. Who says personas can't dance? The use of comic strips to design information security personas. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2485–2490.

[27] Neil Finlay MacEwan. 2017. *Responsibilisation, rules and rule-following concerning cyber security: findings from small business case studies in the UK*. Ph.D. Dissertation. University of Southampton.

[28] Sally Maitlis and Scott Sonenshein. 2010. Sensemaking in crisis and change: Inspiration and insights from Weick (1988). *Journal of management studies* 47, 3 (2010), 551–580.

[29] Luciana Andréia Fondazzi Martimiano and Edson dos Santos Moreira. 2006. The evaluation process of a computer security incident ontology. In *Workshop on Ontologies and their Applications (WONTO)*. CEUR Workshop Proceedings, CEUR-WS.org.

[30] Ruth Massie. 2015. *Allocating effort: risk and complexity in board directors' engagement with information*. Ph.D. Dissertation. City University London.

[31] Sammy Migues. 2021. Crossing the security poverty line. https://www.forbes.com/sites/forbestechcouncil/2021/09/14/crossing-the-security-poverty-line/

[32] Stuart Mills. 2020. Personalized nudging. *Behavioural Public Policy* (2020), 1–10. https://doi.org/10.1017/bpp.2020.7

[33] Tyler Moore, Scott Dynes, and Frederick R Chang. 2016. Identifying how firms manage cybersecurity investment. *15th Annual Workshop on the Economics of Information Security (WEIS 2016)* (2016).

[34] Mary S Morgan. 2014. Resituating knowledge: Generic strategies and case studies. *Philosophy of Science* 81, 5 (2014), 1012–1024.

[35] Kennedy Njenga and Pierre Jordaan. 2016. We want to do it our way: The neutralisation approach to managing information systems security by small businesses. *The African Journal of Information Systems* 8, 1 (2016), 3.

[36] Calvin Nobles and Darrell Burrell. 2018. Using Cybersecurity Communities of Practice (CoP) to Support Small and Medium Businesses. In *ICIE 2018 6th International Conference on Innovation and Entrepreneurship: ICIE 2018*. Academic Conferences and publishing limited, 333.

[37] Donald Nordberg and Rebecca Booth. 2019. Evaluating the effectiveness of corporate boards. *Corporate Governance: The international journal of business in society* (2019).

[38] Emma Osborn. 2015. Business versus technology: Sources of the perceived lack of cyber security in SMEs. *Centre for Doctoral Training (CDT) in Cyber Security (Oxford University) Technical Paper 01/15* (2015).

[39] Emma Osborn and Andrew Simpson. 2018. Risk and the small-scale cyber security decision making dialogue—a UK case study. *Comput. J.* 61, 4 (2018), 472–495.

[40] Simon Parkin, Andrew Fielder, and Alex Ashby. 2016. Pragmatic security: modelling it security management responsibilities for SME archetypes. In *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*. ACM, 69–80.

[41] Simon E Parkin, Aad van Moorsel, and Robert Coles. 2009. An information security ontology incorporating human-behavioural implications. In *Proceedings of the 2nd International Conference on Security of Information and Networks (SIN '09)*. ACM, 46–55.

[42] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E Grinter, and W Keith Edwards. 2009. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 739–748.

[43] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (2015), 121–144.

[44] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. USENIX Association, 1–17.

[45] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the Web. In *29th USENIX Security Symposium (USENIX Security '20)*. USENIX Association, 89–108.

[46] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64.

[47] Karen Renaud and Marc Dupuis. 2019. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop (NSPW)*. ACM, 42–56.

[48] Karen Renaud and George RS Weir. 2016. Cybersecurity and the unbearability of uncertainty. In *2016 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 137–143.

[49] Grace Ann Rosile, David M Boje, Donna M Carlon, Alexis Downs, and Rohny Saylors. 2013. Storytelling diamond: An antenarrative integration of the six facets of storytelling in organization research design. *Organizational Research Methods* 16, 4 (2013), 557–580.

[50] Kenneth Albert Saban, Stephen Rau, and Charles A Wood. 2021. SME executives' perceptions and the information security preparedness model. *Information & Computer Security* (2021).

[51] Edgar H Schein and Peter A Schein. 2021. *Humble inquiry: The gentle art of asking instead of telling*. Berrett-Koehler Publishers.

[52] Zur Shapira. 1995. *Risk taking: A managerial perspective*. Russell Sage Foundation.

[53] Jonathan M Spring and Phyllis Illari. 2019. Building general knowledge of mechanisms in information security. *Philosophy & Technology* 32, 4 (2019), 627–659.

[54] Jonathan M Spring, Tyler Moore, and David Pym. 2017. Practicing a science of security: a philosophy of science perspective. In *Proceedings of the 2017 New Security Paradigms Workshop (NSPW)*. ACM, 1–18.

[55] Joe Tidy. 2021. The ransomware surge ruining lives. https://www.bbc.com/news/technology-56933733

[56] Tommy van Steen, Emma Norris, Kirsty Atha, and Adam Joinson. 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity* 6, 1 (2020), tyaa019.

[57] Rick Wash and Molly M Cooper. 2018. Who provides phishing training? facts, stories, and people like me. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. ACM, 1–12.

[58] Rick Wash and Emilee Rader. 2015. Too much knowledge? Security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, 309–325.