Industrial and Organizational Psychology, 11(2), pp 346–365 June 2018.
 doi:10.1017/iop.2018.3

Practice Forum

The Looming Cybersecurity Crisis and What It Means for the Practice of Industrial and Organizational Psychology

Rachel C. Dreibelbis
Jaclyn Martin
Michael D. Coovert
University of South Florida

David W. Dorsey
Human Resources Research Organization

The persistently changing landscape of cyberspace and cybersecurity has led to a call for organizations' increased attention toward securing information and systems. Rapid change in the cyber environment puts it on a scale unlike any other performance environment typically of interest to industrial and organizational (I-O) psychologists and related disciplines. In this article, we reflect on the idea of keeping pace with cyber, with a particular focus on the role of practicing I-O psychologists in assisting individuals, teams, and organizations. We focus on the unique roles of I-O psychologists in relation to the cyber realm and discuss the ways in which they can contribute to organizational cybersecurity efforts. As highlighted throughout this article, we assert that the mounting threats within cyberspace amount to a "looming crisis." Thus, we view assisting organizations and their employees with becoming resilient and adaptive to cyber threats as an imperative, and practicing I-O psychologists should be at the forefront of these efforts.

Keywords: cybersecurity, selection, data security

Although once relegated to the pages of science fiction novels,[1] the ideas of "cyber," "cyberspace," and "cybersecurity" have become present reali-

Rachel C. Dreibelbis, University of South Florida; Jaclyn Martin, University of South Florida; Michael D. Coovert, University of South Florida; David W. Dorsey, Human Resources Research Organization.

All statements expressed in this article are those of the authors and do not reflect the official opinions or policies of the United States government.

Correspondence concerning this article should be addressed to Rachel Dreibelbis, University of South Florida, 4202 E. Fowler Ave., Tampa, FL 33620. E-mail: rdreibelbis@mail.usf.edu

[1] Cyberspace as a term might have been first coined by the science fiction author William Gibson in his short story "Burning Chrome." Others (e.g., Gutzwiller, Fugate, Sawyer, & Hancock, 2015) suggest that the idea of cyberspace might have been inspired by Norbert Wiener's work on cybernetics (Wiener, 1961).

ties. The terms cyber or cyberspace correspond to "The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems and embedded processors and controllers" (UMUC, 2016). More or less, it is everything that happens once you interact with a computer, personal electronic device, or connected "thing" (as in the Internet of Things). The cybersecurity aspect of cyber is exactly what it sounds like: securing information, systems, or other valuable commodities from exploitation, theft, or manipulation via electronic means.

Today, we are in the Wild West of cyber maturation. Changes in cyberspace are driven by a unique interplay of technologies, companies, individual actors, governments, and academic institutions. This makes the cyber environment volatile on a scale unlike any other performance environment typically of interest to industrial and organizational (I-O) psychologists and related disciplines. Even when compared to other complex human–machines systems (e.g., military systems), the pace and the nature of change in cyber domains are beyond those experienced before. In a matter of hours or even minutes, vulnerability can be discovered, a zero-day exploit released, or a hack initiated; any of these can fundamentally alter the marketplace of information and systems that define much of modern society.

Part of this volatility is driven by the exponential nature of today's technological development. Exponential technologies are drastically changing the modern world, often with unexpected consequences (Briggs & Shingles, 2015). These technologies disrupt prior operating paradigms in society (Briggs & Shingles, 2015), often under the promise of new opportunities, advances, and conveniences.

Despite the presumed advantages, the growth of exponential technologies introduces discontinuities that are nearly impossible to predict. In addition, many of the technologies that are developed are brittle, in the sense that security and related considerations are often afterthoughts. The longstanding preference of individuals for usability over security has plagued technology development for decades (Andriotis, Tryfonas, & Oikonomou, 2014). Central to this preference is the fact that users often do not consider themselves to be at risk (West, 2008). This dynamic has led to the usability–security tradeoff myth, which says that organizations assume that in order to ensure security, they must sacrifice usability (Sasse, Smith, Herley, Lipford, & Vaniea, 2016). This assumption fails to consider that the idiosyncrasies of human behavior should be considered in this era of technology development instead of ignored.

This ever-changing technical landscape makes it difficult for scientists, organizations, and especially practitioners to keep up. In this article, we reflect on this idea of maintaining pace with cybersecurity, with an emphasis

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

on the role of practicing I-O psychologists in assisting individuals, teams, and organizations. As highlighted throughout this article, we believe the mounting threats within cyberspace amount to a "looming crisis." Thus, we view assisting organizations and their employees with becoming resilient and adaptive to cyber threats as imperative.

In this article we focus on the unique roles of practicing I-O psychologists in cybersecurity and how they can meaningfully contribute to and influence the security of information in cyberspace, both at an individual and organizational level. In the cybersecurity era we require an *exponential psychology* to keep up with exponential technologies. I-O practice needs be at the forefront of such efforts.

Organizational Practice Interventions

The exponential growth of the various types of threats that occur from multiple sources (e.g., malware, physical information loss, network threats) has resulted in an increased need to evaluate such dangers from perspectives beyond computers and security. Technology does not exist in isolation from humans, so it is prudent to consider the human element and its interaction with information technology (Pfleeger & Caputo, 2012). For example, consider a piece of malware; it originates from a human's computer and relies on another human's (the target's) vulnerability to achieve a goal. Although the attacker and target may never meet in person, they interact through their machines, and by proxy, each other. Space constraints prohibit us from providing a rich discussion of cyber threats; we therefore provide a brief description in Table 1.

The nature of interactions between attacker and target, and of questions surrounding them, has led to the emergence of a new hybrid in cybersecurity and psychology, coined "cyberpsychology." The cyberpsychology domain considers human existence within the context of our own digital tools and how we interact in a digital space (Norman, 2008). Practitioners in this field are investigating a wide range of topics, such as the use of social media by end users and adversaries, cyber actor profiling, raising public awareness of cybersecurity risks, and changing behaviors about privacy (Wiederhold, 2014). Although the roles of the practicing I-O psychologists in the cyber domain have yet to fully emerge, we now begin to explore this critical issue.

We discuss potential I-O psychology–based practice interventions in much the same way that organizations experience the flow of employees and information—inputs, throughputs, and outputs. First, we discuss how we, as practicing I-O psychologists, can understand the task/job environment of both cybersecurity professionals and end users—how we can influence and mold cybersecurity selection research and development, and highlight challenges to combatting information loss during the selection process.

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

Table 1. Types of Attackers

Type of threats	Motivation (ultimate goal)	Example
Organized attackers (espionage, terrorism, warfare)	• Loss of life • Economic turmoil • Disruption of operations	• Anonymous group's hacks on the Church of Scientology.
Employees (insider threat, disgruntled employees)	• Maliciousness • Personal or financial gain • Ideological change • Carelessness (unintentional harm)	• An employee creates a backdoor for an outside hacker to utilize. • An employee sends sensitive, unencrypted information through email.
Professional hackers (black hat, grey hat)	• Maliciousness • Personal or financial gain	• An individual sponsored by a foreign agent exploits weaknesses in an organization's system in order to steal employees' identifying data.
Amateurs	• Maliciousness • Personal or financial gain	• An individual sends a phishing email to an employee's computer to gain access to login information and customer credit card information.

We then move on to organizational processes, such as I-O interventions for mitigating insider threat, and the importance of building and sustaining an effective cybersecurity culture in organizations. Last, we discuss outputs of these efforts, such as how organizations can become adaptive to threats through breach prevention and response.

The Cybersecurity Job Environment

I-O psychologists typically regard job analysis as the building block of all other activities and functions that we perform in an organization. Job analysis is used to identify essential functions and KSAOs (knowledge, skills, abilities, and other characteristics) necessary to perform job functions and to develop performance criteria (Ash & Levine, 1980; Brannick, Levine, & Morgeson, 2007). This same principle can, and should, be applied to the cybersecurity domain. In order to adequately select and train for successful cybersecurity performance at individual, team, and organizational levels, we first must understand the task environment for cybersecurity professionals and end users.

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

Cybersecurity is considered a subset of information security but remains unique in that cybersecurity focuses on defending data specifically in the cyber realm (i.e., the Internet), whereas information security is concerned with protecting both electronic and physical information (Buchy, 2016). We focus specifically on cybersecurity jobs in this discussion but also note that I-O psychologists should consider end users and their behavior as well. There is currently little consistency in the public and private sectors in how cybersecurity work roles are named, defined, and described (National Cybersecurity Workforce Framework, 2016). By using a common language to describe this work, practitioners can identify skill gaps in organizations and design and implement tools to effectively select and train these professionals.

The National Initiative for Cybersecurity Education (NICE) proposed the National Cybersecurity Workforce Framework, which provides a common structure for describing all cybersecurity work and workers, regardless of organizational context (National Cybersecurity Workforce Framework, 2016). This framework described jobs in terms of their functional requirements and included 33 specialty areas divided into seven categories (National Cybersecurity Workforce Framework, 2016). Sample job areas include information assurance compliance, systems development, computer network defense analysis, cyber operations, and strategic planning and policy. Campbell, Saner, and Bunting (2016) proposed an alternative structure, the Cyber Aptitude and Talent Assessment (CATA), to describe cybersecurity jobs based on their cognitive, rather than functional, requirements. Campbell et al. (2016) proposed that tasks described in the NICE Cybersecurity Workforce Framework could be plotted along two dimensions: real-time/exhaustive and initiating/responding. Depending on where the tasks for a job fall on those two dimensions, any job can be classified into one of four quadrants (attacking, defending, development, or exploitation). Together, the NICE and CATA frameworks provide useful tools for better understanding the scope of cybersecurity jobs and supplementing job analytic techniques.

Whereas traditional job analysis methods view jobs as relatively stable over time, jobs in the cybersecurity domain tend to evolve quickly, meaning the knowledge, skills, and abilities required 10 years from now for a cybersecurity professional might look very different from the knowledge, skills, and abilities required today (Campbell et al., 2016). For example, U.S. Department of Homeland Security's Federal Emergency Management Agency's (FEMA) computer network defense analyst job position described someone who "uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or may possibly occur within the network" (FEMA, 2016, pp. 1). The defensive measures and sources of information that a computer network defense

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

analyst uses today may look very different in the future, as tools and technology become increasingly sophisticated. Similarly, cybersecurity jobs that do not exist today may be essential to organizational performance or security in a few brief years.

As such, strategic job analysis (SJA; Schneider & Konz, 1989) may be especially appropriate for cybersecurity jobs, because this technique describes the current state of the job and also anticipates performance requirements of jobs that will exist in the future. SJA has been successfully used in both private and public sectors to identify tasks that are critical for future job performance (Kolmstetter, 2003; Landis, Fogli, & Goldberg, 1998; Sager, Russell, Campbell, & Ford, 2005). Practitioners must be aware of this increased complexity when conducting job analysis and should choose appropriate job analysis methods that explicitly take dynamic changes in work requirements into account. For example, a practitioner may choose to generate categories of technology knowledge (metaknowledge or knowledge ontologies) rather than specific exemplars, as the specific toolsets used in any given technology domain may change unabatedly. Moreover, due to the inherently cognitive and human–computer mediated nature of cybersecurity work, nontraditional job analytic techniques may be particularly useful, including methods such as cognitive interviews, system observations, and even sorting activities (e.g., Paul & Whitley, 2013). Cognitive task analysis (CTA) is also a nontraditional job analysis method that is typically used in the realm of performance appraisal and training, which could offer insight into the cognitive nature of KSAOs for cybersecurity professions and also offers untapped application within the realm of selection (Brannick, Pearlman, & Sanchez, 2017; Gordon et al., 2001). Brannick et al. (2017) posited that CTA is particularly useful in the domain of selection for creating work samples, specially constructed simulations, and situational judgment tests (SJTs) for cognitively loaded occupations. Capturing meta-cognition is also likely a key aspect of understanding job requirements. For example, as exemplified by Paul and Whitley (2013), job analysts should reflect on the questions that cybersecurity analysts or cybersecurity operators ask themselves during a cybersecurity event. Recent studies of network operations centers (Paul, 2014) and work requirements for duties such as attack detection (Ben-Asher & Gonzalez, 2015) suggest that our comprehension of these environments is in an infantile state.

When striving to understand the cybersecurity task environment, we necessarily also consider end-users. Although end-users' primary job responsibilities do not involve information security of any kind, if they are not vigilant about protecting information at work, end users present a critical threat vector (Guo, Yuan, Archer, & Connelly, 2011). This is particularly problematic as employees do not typically consider cybersecurity behavior as

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

part of their job (Albrechtsen, 2007), and such views may be a key reason for employee cybersecurity misbehavior. From a job analysis perspective, now perhaps more than ever, technology use and the responsibilities that come with that use should be viewed as a job responsibility.

To summarize, I-O psychology practitioners should take the changing nature of technology and cybersecurity environments into account when identifying the competencies and KSAOs required for both cybersecurity professionals and end users.

Cybersecurity Selection Research and Development

A robust cybersecurity strategy begins with selecting the right people to identify, build, and protect an organization's cyber defense systems. The reality is, however, that finding and selecting the right talent is more challenging than ever. According to the results from the eighth Global Information Security Workforce Study (GISWS), the demand for cybersecurity professionals is expected to reach over 6 million globally by 2022, with a projected shortage of 1.8 million qualified professionals (Forrest & Campbell, 2017). This is an almost 20% increase from the 1.5 million projected shortage by the 2015 GISWS. Although these numbers are bleak and problematic for the future of cybersecurity, I-O psychology practitioners are in a unique position to aid organizations in developing new ways to attract and select the best talent.

Practitioners have recently recommended a multipronged approach to cybersecurity for hiring and retaining cybersecurity personnel that considers both distal (e.g., cognitive ability, personality) and proximal characteristics (e.g., social skills, technical knowledge; Jose, LaPort, & Trippe, 2016). There is a growing body of literature surrounding the antecedents of insider behavior (e.g., Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath and Rao, 2009; Hu, Dinev, Hart, & Cooke, 2012), yet there is still a need to understand the predictors of job success for cybersecurity professional jobs. Research has shown that successful cyber operators need knowledge of technology and information systems as well as the ability to learn and adapt (Ben-Asher & Gonzalez, 2015; Evans & Reeder, 2010). Perhaps less explored is the likelihood that these operators need a unique combination of personality and motivation to thrive on the job. Given that practitioners have started building frameworks to incorporate personality in order to identify insider and outsider threats (Greitzer & Frincke, 2010), it may be prudent to integrate more facet-based approaches, based on criterion-correspondence, to gain additional predictive utility over traditional predictors such as job knowledge and cognitive ability. Given the dynamic and demanding nature of cybersecurity roles, it is possible that some roles are more prone to within-person variability in performance (Mueller-Hanson & Garza, 2016). Although little research has addressed this topic in the context of cybersecurity thus far, it

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

would be prudent to focus on within person variability as a consideration when identifying individual differences needed for successful performance over time.

Additionally, many cybersecurity professions are team based, making best practices of teamwork a key component to understanding how to select and construct effective cybersecurity teams (Mancuso et al., 2014). There are also ethical considerations for hiring and selecting talented cyber operators. For example, hackers within an organization can easily use their skills for altruistic (white hat hackers) or malicious purposes (black hat hackers)—or somewhere in between (grey hat hackers). Therefore, it is critical to consider the motivations of cyber operators during the selection process in order to reduce the risk of insider threat. Other potential unique individual difference components of cybersecurity jobs include elements such as the need for extreme vigilance (an attribute well-studied in the human factors literature) and the possibility of working in an environment with poor feedback (Gutzwiller et al., 2015).

The shortage of cybersecurity professionals is not solely a selection problem; it is also one for recruiting and training. Hackers and those who can effectively prevent hacks are not currently coming through traditional education pipelines such as universities, especially with the growing popularity of free or lower cost software development training programs (Moon, 2012). Therefore, organizations need to exploit nonconventional talent pools. Federal agencies have begun to follow this new model, by attending events like DefCon, one of the world's largest hacker conferences, in order to recruit talent (Smith, 2011). Because some of the smartest, most talented individuals might not hold a college degree, organizations need to recruit from high schools and technical schools. These individuals have the ability to learn basic information systems knowledge; therefore, organizations can provide on the job training for specific skills. Although this process initially might be more costly, employee investment and training can lead to increased perceptions of organizational justice (Meyer & Allen, 1997), which can help organizations attract and retain top cybersecurity talent.

Cybersecurity Obligations in I-O Psychology Practice

An often overlooked area of action for I-O psychologists is their role in data security in the cyber realm, both within their own organizations and for their clients. Given the nature of the work, both internal practitioners and external consultants often have access to and collect private, sensitive information on job candidates and incumbents, middle managers, and senior leadership potentially from multiple states and countries. According to a survey of 149 I-O psychologists during SIOP's Leading Edge Consortium in 2009, 87% indicated that their organization collects personal information over the Internet

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

(Reynolds, 2010), and that percentage is likely even higher today. As soon as this information is collected in the cyber realm, it becomes a cybersecurity risk, subject to cyberattacks and therefore subject to privacy and safety regulations put forth by both the United States and the European Union. Despite these regulations, many I-O psychologists seem unaware of if their organizations are taking the necessary steps to protect that information. In that same survey, 71% of I-O psychologists indicated that they were not sure if their assessments were compliant with the latest European Union data protection regulations, and 63% said they were unsure if their organization was registered with the U.S. Safe Harbor Program (now the Privacy Shield program; Reynolds, 2010).

The most recent directive regarding data privacy was set forth by the European Union's General Data Protection Regulations (GDPR), which affect any data originating in the EU or from EU citizens. These regulations outline specific minimum data protection requirements for personal data (e.g., IP address) and sensitive personal data (e.g., home address, birthday) for any companies within the EU. The regulations require organizations to understand and document the information they have, who can access this information, and where the information is stored (Kerner, 2017). These regulations are set to have a global impact, and according to the GDPR Preparedness Pulse Survey conducted by Pricewaterhouse Coopers, 92% of U.S.-based multinational corporations consider compliance with GDPR regulations a top priority (Pricewaterhouse Coopers, 2017). With these regulations going into effect May 2018, organizations dealing with any European data must comply with these regulations or face a 4% fine of global revenues (Boulton, 2017). Additional information for these regulations can be found at www.eugdpr.org. U.S.-based organizations also have the option of registering as privacy shield organizations under the U.S. Department of Commerce, which formally declares that they are in compliance with EU regulations ("Privacy Shield Program Overview," n.d.).

Given the legal risk associated with the nature of digital data collection, these regulations touch every aspect of the work done by I-O psychologists, including recruitment, selection, training, and development and coaching programs. Suppose a U.S.-based psychologist designs a coaching and evaluation program for top executives at a multinational organization with offices in the United States and Europe. Personal information, multirater survey responses, performance reports, and feedback documentation are transmitted via email across country lines, making information on the European executives subject to European data privacy regulations. If this data were to be stolen via cyberattack, the psychologist and his or her organization would not only be subjected to legal fines and prosecution, but also could face severe damage to the client's trust and reputation. Although this is merely one

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

illustrative example, the same scenario could be applied to any I-O psychology practitioner dealing with information stored in a digital format. Therefore, it is critical that I-O psychologists adhere to the same cybersecurity precautions they espouse to their internal and external clients. Reynolds (2010) outlines actionable items for I-O psychologists and HR professionals to increase compliance with privacy regulations, which we feel are important to highlight as they are highly relevant to cybersecurity. Reynolds (2010) recommends designating data collection systems for increased privacy control; collecting only predetermined, necessary information; defining data policies in advance to determine who will have access to private information; carefully documenting when and why data transfers are necessary; and reviewing security practices specifically regarding the use of technology that may contain personally sensitive information. We further elaborate some of these recommendations in the context of intellectual property in the following section.

Counteracting Intellectual Property Loss

From an economic standpoint, theft of intellectual property (IP) is one of the most financially devastating attacks because it can have long-term effects (Andrijcic & Horowitz, 2006). As a nation, the U.S. loses hundreds of billions of dollars a year through IP theft; the scale of loss is so large it matches the size of U.S. exports to Asia (The IP Commission, 2013).

An example of IP loss particularly relevant to I-O psychology is the loss of test or user information/content during online testing. Clearly, organizations rely on the integrity of test takers to effectively select individuals for hiring, but when the very platforms hosting assessment vehicles are unsecure, organizations run the risk of invalidating their selection tools. Aside from increased access to tests through online platforms, "brain dumping" represents another threat to the information security of assessments (Cholez, Mayer, & Latour, 2010). This process involves test takers memorizing test items in order to "dump" the information on a forum to share with future takers of the test. For example, through collective efforts and time, a group of student test takers in China were able to replicate not only one version of the GRE (Graduate Record Exam) but the entire test bank with incredible accuracy (Dorsey, Martin, Howard, & Coovert, 2017; Smith & Prometric, 2004).

How might the I-O practitioner help address the threat of IP loss? In terms of prevention, implementing remote proctoring protocols can help, though more research is needed on what these methods might entail (e.g., video proctoring, warnings; Tippins, 2009). In addition, organizations have started to evolve advanced forensic methodologies for combating online theft/cheating. For example, Gibson and Mulkey (2016) presented several

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

techniques for using data forensics to identify stolen or compromised test material and responses. Advances in the field of automatic item generation might also help address the brain dump issue (Arendasy & Sommer, 2012). Additionally, as with all cyber threat prevention, organizations should implement two important procedures. First is deploying the necessary software for malware prevention, and second is to ensure cybersecurity teams work on monitoring traffic to the organization's networks and perform appropriate forensics.

Still, breaches occur for companies with even the most advanced security measures, so organizations must be prepared for breach response. I-O practitioners should be part of the breach response team. Components of effective breach response include obtaining appropriate resources required to identify the source of intrusions, handling the compromised information systems (IT department), mitigating resulting reputation damage (public relations firms), and pursuing justice (lawyers, forensics teams; see U.S. Department of Justice, 2015; Dorsey et al., 2017).

Understanding Insider Threat

As previously mentioned, though they may be the first that come to mind, outsiders are not the only threat to organizations. The majority of cybersecurity threats come from an internal source: an employee. Internal threats vary on their degree of malicious intent to harm the organization, such that while certain behaviors are used to purposefully leak sensitive organizational information, other behaviors merely reflect laziness or naïveté, each of which can result in noncompliance with cybersecurity procedures. Insider threats are especially concerning for organizations because employees already have access to the organization's information systems and servers (Coovert, Dreibelbis, & Borum, 2016). Consequently, this is an area where interventions and tools from I-O practitioners can be particularly useful.

There are two different philosophies for how to approach insider threat: (a) *prevent them* or (b) *catch them*. Preventing insider threats could involve trying to select individuals who are less likely to pose a cybersecurity threat or implementing training interventions to decrease the risk of susceptibility to social engineering. If cybersecurity behaviors are a form of counterproductive work behaviors (CWBs), there is the possibility that personality tests would be helpful in predicting an individual's cybersecurity performance (Motowidlo, Borman, & Schmit, 1997). For most employees who pose a nonmalicious threat, cybersecurity tasks (even small things like looking out for phishing emails) might have been part of their onboarding training, though it is likely not part of an official job description. As such, cybersecurity behaviors should be considered an emerging class of extra-role or organizational citizenship behaviors (OCBs), signaling the importance of

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

citizenship-related predictors. In fact, there is preliminary research that suggests that personality predicts phishing susceptibility; the results, however, are mixed (El-Din, Cairns, & Clark, 2015; Parrish Jr., Bailey, & Courtney, 2009; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010; Vishwanath, 2015).

From a training perspective, if organizations can predict individuals who are likely to violate cybersecurity procedures, they should focus cybersecurity training efforts on the identified individuals. More research is needed to identify the most effective methods of cybersecurity training, but simulations and avatar training could provide less abstract, higher fidelity options that might increase effectiveness. Another method for preventing insider threat involves adopting a security culture. Similar to the occupational health and safety literature (Beus, Payne, Bergman, & Arthur Jr., 2010; Clarke, 2006), a security climate would greatly reduce the number of incidents. Organizations should focus training efforts on those individuals who deal with more sensitive information. For instance, the human resources department has personally identifiable information (social security numbers, bank accounts, etc.) for all the organization's employees. Therefore, it is especially important that those employees are assessed for and well trained in cybersecurity protocols.

Another concern within insider threat lies in the ubiquitous use of social media. Through social media, people have a greater ability than ever to share information. Because employers cannot control the information that employees share when they are not at work, they cannot prevent related consequences. Though employers may be able to ensure that employees do not share confidential organizational information (through contracts, and so forth), they cannot prevent employees from sharing personal information. Personal information on public media helps adversaries gather information on individuals in order to create a more convincing social engineering attack (Jagatic, Johnson, Jakobsson, & Menczer, 2007). For instance, a hacker might use someone's Facebook page to find information on their interests and friends in order to draft a believable phishing email that appears to be from a friend and is asking the individual to read over a draft of their report. Moreover, adversaries can mimic popular social media sites in order to acquire an individual's login information, which people frequently replicate on work-related systems. The I-O practitioner can play a central role in developing policies and procedures, selection, and training in the use of social media by employees in and out of the workplace.

Building a Security Culture

When an organization experiences a security breach or even a threat of an attack, a common reaction is to implement stronger security policies.

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

Although these policies might make employees more aware of the rules surrounding their behavior, they do not guarantee that employees become more "cyber safe" (Guo et al., 2011). In fact, one study found that employees continued to allow others to use their computers, despite being aware this compromised the security of their systems (Dubie, 2007). Although it is not clear why employees knowingly break the rules, some research suggests that organizational norms, culture, and top management behavior all influence cyber-safe or cyber-risky behavior (Guo, 2013; Guo et al., 2011; Hu et al., 2012; Padayachee, 2012). Further, researchers have noted that establishing an information security culture is a key component for organizations to have effective information security (Eloff & von Solms, 2000; von Solms, 2000).

I-O psychology practitioners can contribute to the improvement of security climate/culture in various settings by working toward the integration of security into everyday work. If employees perceive that information security is expected and visible at all levels of the organization, the organization as a whole has the potential to become more secure (Van Niekerk & von Solms, 2010).

Organizational Threat Adaptation

Thus far, we have discussed I-O psychology intervention from primarily the input and throughput stages; however, the process is deficient while it ignores the organizational outcomes related to these efforts. Each of these efforts, including task analysis, selection, identification of insider threats, and a strong security culture, can be contributed to by the I-O psychology practitioner to help build organizations that are adaptive to the constantly evolving threats presented in the world today. Consensus among security firms suggests that the typical "parameter defense" posture taken by many organizations is no longer effective, and organizations should embrace the evolving cyber ecosystem that can increase "cyber resilience" (EY, 2014). In a report on building organizational resilience in the cyber domain, EY Corporation identified four key attributes that can help organizations adapt and anticipate security threats: resilient leadership, resilient culture, resilient networks, and resilient change readiness. Many of the recommendations focus on people: specifically, the construction of teams that are equipped with the training and tools to "rapidly detect, respond to and adapt security responses in an ever changing security context" (EY, 2014, p. 10). These areas are often the core competencies of the I-O practitioner. Furthermore, the growing literature on organizational adaptability (Ployhart & Turner, 2014) in general may also be helpful to the I-O practitioner in building organizations that are adaptive to cyber threats.

Teams and virtual teams research is plentiful in the current literature, but much of the research on effective cybersecurity teams has been confined

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

to military and government settings. For example, Champion and colleagues found that encouraging analysts to work as a team and providing team rewards lead to increased performance, but team structure, a lack of team communication, and information overload all contributed to the degradation of cybersecurity team performance in a cybersecurity defense task (Champion, Rajivan, Cooke, & Jariwala, 2012; Rajivan et al., 2013). This research has provided insight into understanding the complexities involving cybersecurity teams and can be exploited by I-O practitioners to help employees develop the skills and training required to anticipate and react effectively to cyber events. Understanding these teams, as well as effective employee selection, training, and culture, will create a more agile organization.

Summary of Areas for Practice

As discussed in the sections above, I-O psychologists have ample opportunity to contribute to the success of organizations' evolving cybersecurity strategies. Table 2 summarizes the points discussed in the previous sections. We intend the ideas listed here to serve as areas for practitioners to expand I-O psychology's influence in cybersecurity by making immediate contributions to practice and to serve as boundary spanners and further facilitate research for practice contributions.

With the increasingly connected workplace, where there is a greater portion of work relying on interface with the Internet and there are more virtual employees than ever before, it is important to not only consider changes to the organization with the onboarding of more cybersecurity professionals, but also the changes necessary to ensure cybersecurity with all end-users. In the area of job and work analysis, this means appropriately matching job analysis techniques to the nature of cybersecurity-related jobs as well as incorporating cybersecurity compliance tasks into job analyses for an increasing number of other jobs (namely any role that is connected and is therefore at risk for cyberattack). Similarly, for selection purposes, the specific cybersecurity knowledge, skills, abilities, motivation, and fit need to be considered for both cybersecurity professionals and end-users. Additionally, all selection tests should be properly secured when distributed to avoid IP and data loss.

In terms of training, not only is it imperative to properly train cybersecurity professionals, but end-users also should be continuously trained on how to recognize and handle cybersecurity threats. This training would reduce the incidence of insider threat. The IT and cybersecurity professionals should ensure that the organization builds a cybersecurity culture and facilitates organizational adaption of cybersecurity policies, norms, and standards. Keeping end-users abreast of current cybersecurity threats and ways to work together to combat the threats is one step toward this goal. For

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

Table 2. Areas for the I-O Practitioner to Immediately Contribute and Facilitate Future Research

	Practice in these areas	Practice should facilitate research in these areas
Job and work analysis	• Consider appropriate job analysis techniques to account for the changing nature of cyber jobs. • Incorporate cybersecurity policy and responsibilities into end user job requirements according to organizational policies.	• Expand and refine existing frameworks for cyber jobs. • Investigate the utility of strategic and cognitively oriented job analysis techniques for cyber related work roles.
Cyber selection	• Select for specific cyber skills, knowledge, motivation, and fit. • Understand the ethical motivations behind hackers and cyber professionals. during the hiring process. • Consider nontraditional sources for recruitment and selection.	• Investigate the antecedents, particularly personality and motivation, of cybersecurity performance for cyber professionals and end-users. • Model the effects of cybersecurity selection and training on individual- and organizational-level outcomes.
Cybersecurity obligations	• Increase awareness of the risks to electronically stored data. • Ensure that sensitive data is secured and compliant with EU data regulations.	• Develop methods of assessment and data analysis techniques that can minimize the necessity for personally identifiable data.
Counteracting IP loss	• Make sure Internet selection tests are properly proctored and secured. • Closely monitor web traffic and the Internet for signs of breaches or stolen material. • Ensure that there is response protocol, should intellectual property be stolen.	• Assess the damage that intellectual property theft can have on an organization's reputation. • Develop effective responses to breaches in terms of public response and outreach after a breach.
Insider threat	• Select for individuals who are less likely to pose a threat. • Develop training programs to reduce insider threats.	• Examine the potential antecedents for each malicious and nonmalicious insider threats.

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

Table 2. Continued

	Practice in these areas	Practice should facilitate research in these areas
	• Consider methods for identifying individuals who need targeted cybersecurity training.	• Determine the utility of different selection tools. and/or interventions for reducing insider threat.
Growing a cybersecurity culture	• Work toward integrating the acceptance of cyber safe behaviors in the workplace at all management levels. • Build an internal security climate/culture.	• Further explore the antecedents and consequences of organizational cyber culture. • Develop psychometrically sound measures for assessing cyber culture, exploring possible facets of cyber culture.
Organizational adaptation	• Create organizational policies, norms, and standards for employee responses to cybersecurity threats and breaches. • Build and select for agile cyber teams.	• Investigate the factors that promote and inhibit successful cyber team performance. • Explore the relationship between cyber selection, training, and culture on organizational level outcomes, such as organizational adaptiveness to cyber threat.

instance, after the recent WannaCry ransomware attack, informing employees on the status of the attack (what it is, who has been affected) and instructing them on what they should do (e.g., open emails carefully, restart system weekly to ensure updates are complete) are instrumental in avoiding system compromise.

Conclusion

What once began as ideas relegated to science fiction and philosophical discussions of human–machine systems (i.e., cybernetics) has now emerged as major facets of modern organizational life. Cyberspace and cybersecurity are areas of inquiry and practice that are here to stay. As outlined in this article, I-O psychology and its adjacent fields of study have important opportunities to impact modern organizational life. Here, we have surveyed a sample of the ways in which I-O practitioners can help to build organizations that both survive and flourish in the periodization of cyber threats and influence.

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

By utilizing what we know and exploiting future developments, the I-O psychology practitioner can facilitate how organizations approach job and work analysis, select for key cybersecurity jobs, counteract IP loss, understand and mitigate insider threat, grow a cybersecurity culture, and facilitate organizational adaptation. We hope this article spurs forward in cyberspace an active embrace among employees, organizations, and I-O psychology practitioners.

References

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276–289.

Andrijcic, E., & Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk Analysis*, *26*(4), 907–923.

Andriotis, P., Tryfonas, T., & Oikonomou, G. (2014, June). Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 115–126). Cham, Germany: Springer.

Arendasy, M. E., & Sommer, M. (2012). Using automatic item generation to meet the increasing item demands of high-stakes educational and occupational assessment. *Learning and Individual Differences*, *22*(1), 112–117.

Ash, R. A., & Levine, E. L. (1980). A framework for evaluating job analysis-methods. *Personnel*, *57*(6), 53–59.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51–61.

Beus, J. M., Payne, S. C., Bergman, M. E., & Arthur, W. Jr. (2010). Safety climate and injuries: An examination of theoretical and empirical relationships. *Journal of Applied Psychology, 95*(4), 713–727.

Boulton, C. (2017, January 26). U.S. companies spending millions to satisfy Europe's GDPR. *CIO*. Retrieved from https://www.cio.com/article/3161920/privacy/article.html.

Brannick, M. T., Levine, E. L., & Morgeson, F. P. (2007). *Job and work analysis: Methods, research, and applications for human resource management*. Thousand Oaks, CA: Sage Publications.

Brannick, M. T., Pearlman, K., & Sanchez, J. I. (2017). Work analysis. In J. L. Farr & N. T. Tippins (Eds.), *Handbook of employee selection* (pp. 134–162): New York, NY: Routledge.

Briggs, W., & Shingles, M. (2015). Exponentials. Deloitte University Press. Retrieved from http://dupress.deloitte.com/dup-us-en/focus/tech-trends/2015/tech-trends-2015-exponential-technologies.html?id=us:2el:3dc:dup1012:eng:cons:tt15.

Buchy, J. (2016, June 30). Cyber security vs. IT security: Is there a difference? *Cyber Security Degree*. Retrieved from http://business.gmu.edu/blog/tech/2016/06/30/cyber-securit-it-security-difference/.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Campbell, S. G., Saner, L. D., & Bunting, M. F. (2016, April). Characterizing cybersecurity jobs: Applying the cyber aptitude and talent assessment framework. In W. L. Scherlis & D. Brumley (Chairs), *Proceedings of the Symposium and Bootcamp on the Science of Security* (pp. 25–27). New York, NY: ACM.

Champion, M. A., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012, March). Team-based cyber defense analysis. In *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support* (pp. 218–221). Piscataway, NJ: IEEE.

Cholez, H., Mayer, N., & Latour, T. (2010). *Information security risk management in computer-assisted assessment systems: First step in addressing contextual diversity*. Retrieved from http://www.nmayer.eu/publis/CAA10_Information%20Security%20Risk%20Management%20in%20CAA%20Systems.pdf

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

Clarke, S. (2006). The relationship between safety climate and safety performance: A meta-analytic review. *Journal of Occupational Health Psychology, 11*(4), 315–327.

Coovert, M. D., Dreibelbis, R., & Borum, R. (2016). Factors influencing the human-technology interface for effective cyber security performance. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke, (Eds.), *Psychosocial dynamics of cyber security* (pp. 267–290). New York, NY: Routledge.

Dorsey, D. W., Martin, J., Howard, D. J., & Coovert, M. D. (2017). Cybersecurity issues in selection. In J. L. Farr & N. T. Tippins (Eds.), *Handbook of employee selection* (pp. 913–930). New York, NY: Routledge.

Dubie, D. (2007). End users behaving badly. *Network World*. Retrieved from http://www.networkworld.com/slideshows/2007/121007-end-users-behaving-badly.html.

El-Din, R. S., Cairns, P., & Clark, J. (2015). The human factor in mobile phishing. In M. Dawson & M. Omar (Eds.), *New threats and countermeasures in digital crime and cyber terrorism* (pp. 53–65). Hershey, PA: Information Science Reference.

Eloff, M. M., & von Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. *Computers & Security, 19*(3), 243–256.

Evans, K., & Reeder, F. (2010). *A human capital crisis in cybersecurity: Technical proficiency matters*. Washington, DC: CSIS.

EY. (2014, December). *Achieving resilience in the cyber ecosystem*. Retrieved from http://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf

FEMA. (2016, September). Computer network defense analyst. Position qualifications for cybersecurity. Retrieved from https://www.fema.gov/media-library-data/1494503225699-6bbd13419fc3b2e9cf75c397719fb9be/CND_Analyst_509-13_20161020.pdf.

Forrest, M., & Campbell, J. (2017, February 13). Cybersecurity workforce shortage continues to grow worldwide, to 1.8 million in five years. Retrieved June 19, 2017, from https://www.isc2.org/pressreleasedetails.aspx?id=14569.

Gibson, K., & Mulkey, J. (2016). *Dumping the dopes who use braindump sites: How IBM turned the tables using data forensics*. Presented at the 2016 ATP Innovations in Testing Conference, Orlando, FL.

Gordon, T., Coovert, M. D., Miles, D. E., Riddle, D., Elliott, L., & Schiflett, S. G. (2001, June). *Classifying jobs: Integrating cognitive task analysis and verbal protocol analysis*. Paper presented at the annual meeting of the American Psychological Association, Toronto, Canada.

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In C. W. Probst & J. Hunker (Eds.), *Insider threats in cyber security* (pp. 85–113). New York, NY: Springer US.

Guo, K. H. (2013). Security related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242–251.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236.

Gutzwiller, R. S., Fugate, S., Sawyer, B. D., & Hancock, P. A. (2015, September). The human factors of cyber network defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 59, No. 1, pp. 322–326). Thousand Oaks, CA: SAGE Publications.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–659.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100.

https://doi.org/10.1017/iop.2018.3 Published online by Cambridge University Press

Jose, I., LaPort, K., & Trippe, D. M. (2016). Requisite attributes for cyber security personnel and teams: Cyber risk mitigation through talent management. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), *Psychosocial dynamics of cyber security* (pp. 167–193). New York, NY: Routledge.

Kerner, S. M. (2017, May 1). HPE explains what European GDPR privacy regulations mean to U.S. firms. *eWeek*. Retrieved from http://www.eweek.com/security/hpe-explains-what-european-gdpr-privacy-regulations-mean-to-u.s.-firms.

Kolmstetter, E. (2003). I-Os making an impact: TSA transportation security screener skill standards, selection system and hiring process. *The Industrial-Organizational Psychologist, 40*, 39–46.

Landis, R. S., Fogli, L., & Goldberg, E. (1998). Future-oriented job analysis: A description of the process and its organizational implications. *International Journal of Selection and Assessment, 6*(3), 192–198.

Mancuso, V. F., Christensen, J. C., Cowley, J., Finomore, V., Gonzalez, C., & Knott, B. (2014, September). Human factors in cyber warfare II emerging perspectives. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 58, No. 1, pp. 415–418). Thousand Oaks, CA: SAGE Publications.

Meyer, J. P. & Allen, N.J. (1997). *Commitment in the workplace: Theory, research, and application*. Thousand Oaks, CA: SAGE Publications.

Moon, J. (2012). What hacker apprenticeships tell us about the future of education. *The Atlantic*. Retrieved from http://www.theatlantic.com/technology/archive/2012/01/what-hacker-apprenticeships-tell-us-about-the-future-of-education/251039/.

Motowidlo, S. J., Borman, W. C., & Schmit, M. J. (1997). A theory of individual differences in task and contextual performance. *Human Performance, 10*(2), 71–83.

Mueller-Hanson, R. & Garza, M. (2016). Selection and staffing of cyber security positions. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J.A. Steinke (Eds.). *Psychosocial dynamics of cyber security* (pp. 167–193). New York, NY: Routledge.

National Cybersecurity Workforce Framework. (2016, November). *National Initiative for Cybersecurity Education*. Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

Norman, K. L. (2008). *Cyberpsychology: An introduction to human-computer interaction* (Vol. 1). New York, NY: Cambridge University Press.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*, 673–680.

Parrish, J. L. Jr., Bailey, J. L., & Courtney, J. F. (2009). *A personality-based model for determining susceptibility to phishing attacks*. Little Rock, AK: University of Arkansas.

Paul, C. L. (2014, November). Human-centered study of a network operations center: experience report and lessons learned. In *Proceedings of the 2014 ACM Workshop on Security Information Workers* (pp. 39–42). New York, NY: ACM.

Paul, C. L., & Whitley, K. (2013, July). A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 145–154). Berlin/Heidelberg, Germany: Springer.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. *Computers & Security*, *31*, 597–611.

Ployhart, R. E., & Turner, S. F. (2014). Organizational adaptability. In D. Chan (Ed.), *Individual adaptability to changes at work: New directions in research* (pp. 73–92). New York, NY: Routledge.

Pricewaterhouse Coopers. (2017). Pulse survey: US companies ramping up General Data Protection Regulation (GDPR) budgets. Retrieved from https://www.pwc.com/us/en/increasing-it-effectiveness/publications/gdpr-readiness.html.

Privacy Shield program overview. (N.d.). *Privacy shield framework*. Retrieved from https://www.privacyshield.gov/Program-Overview.

Rajivan, P., Champion, M., Cooke, N. J., Jariwala, S., Dube, G., & Buchanan, V. (2013, July). Effects of teamwork versus group work on signal detection in cyber defense teams. In *International Conference on Augmented Cognition* (pp. 172–180). Berlin/Heidelberg, Germany: Springer.

Reynolds, D. (2010, October). A primer on privacy: What every I-O psychologist needs to know about data protection. *The Industrial and Organizational Psychologist, 48*(2). Retrieved from http://www.siop.org/tip/oct10/05reynolds.aspx.

Sager, C. E., Russell, T. L., Campbell, R. C., & Ford, L. A. (2005). Future soldiers: Analysis of entry-level performance requirements and their predictors. Army Research for the Behavioral Sciences, Technical Report 1169. Alexandria, VA: United States

Sasse, M. A., Smith, M., Herley, C., Lipford, H., & Vaniea, K. (2016). Debunking security-usability tradeoff myths. *IEEE Security & Privacy, 14*(5), 33–39.

Schneider, B., & Konz, A. M. (1989). Strategic job analysis. *Human Resource Management, 28*(1), 51–63.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish: A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382). New York, NY: ACM. doi:10.1145/1753326.1753383.

Smith, G. (2011). Feds turn to hackers to defend nation in cyberspace. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/entry/government-recruits-hackers-cyber-shortage_n_920795.

Smith, R. W., & Prometric, T. (2004, April). *The impact of braindump sites on item exposure and item parameter drift*. Paper presented at the annual meeting of the American Education Research Association, San Diego, CA.

The IP Commission. (2013). *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property*. Retrieved from http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

Tippins, N. T. (2009). Internet alternatives to traditional proctored testing: Where are we now? *Industrial and Organizational Psychology, 2*(1), 2–10.

UMUC. (2016). Cyber security primer. University of Maryland University College. Retrieved from http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm.

U.S. Department of Justice. (2015). *Best practices for victim response and reporting of cyber incidents*. Retrieved from https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476–486.

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication, 20*(5), 570–584.

Von Solms, B. (2000). Information security—the third wave? *Computers & Security, 19*(7), 615–620.

West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34–40.

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, *17*(3), 131–132.

Wiener, N. (1961). *Cybernetics or control and communication in the animal and the machine* (Vol. 25). Cambridge, MA: MIT Press.