







SOCIAL ENGINEERING

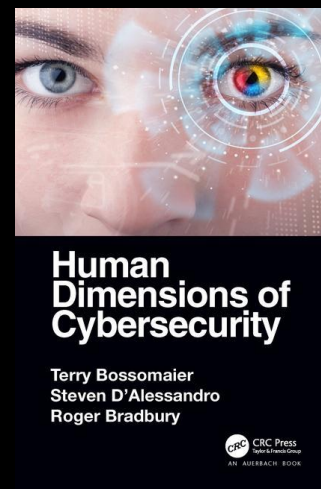
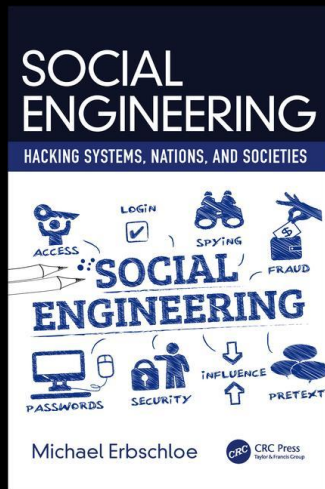
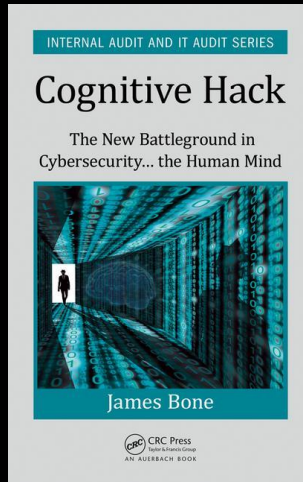
A CRCPRESS FREEBOOK



TABLE OF CONTENTS

-  Introduction
-  1 • Securing Organizations against Social Engineering Attacks
-  2 • Cognitive Behavior
-  3 • The Future

READ THE LATEST ON SOCIAL ENGINEERING WITH THESE KEY TITLES



[CLICK HERE](#)

TO BROWSE FULL RANGE OF CYBERSECURITY TITLES

SAVE 20% AND FREE STANDARD SHIPPING WITH DISCOUNT CODE

FLR40



Introduction

Social Engineering, Hacking Systems, Nations, and Societies analyzes of the use of social engineering as a tool to hack random systems and target specific systems in several dimensions of society. It shows how social engineering techniques are employed well beyond what hackers do to penetrate computer systems. And it explains how organizations and individuals can socially engineer their culture to help minimize the impact of the activities of those who lie, cheat, deceive, and defraud.

Cognitive Hack, The New Battleground in Cybersecurity ... the Human Mind explores a broad cross section of research and actual case studies to draw out new insights that may be used to build a benchmark for IT security professionals. This research takes a deeper dive beneath the surface of the analysis to uncover novel ways to mitigate data security vulnerabilities, connect the dots and identify patterns in the data on breaches.

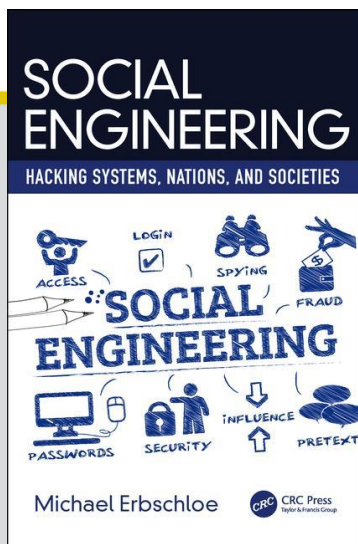
Human Dimensions of Cybersecurity explores social science influences on cybersecurity. It demonstrates how social science perspectives can enable the ability to see many hazards in cybersecurity. It emphasizes the need for a multidisciplinary approach, as cybersecurity has become a fundamental issue of risk management for individuals, at work, and with government and nation states.



CHAPTER

1

SECURING ORGANIZATIONS AGAINST SOCIAL ENGINEERING ATTACKS



This chapter is excerpted from
Social Engineering
Hacking Systems, Nations, and Societies
by Michael Erbschloe

© [2019] Taylor & Francis Group. All rights reserved.

 [Learn more](#)

4

SECURING ORGANIZATIONS AGAINST SOCIAL ENGINEERING ATTACKS

An organization's security culture contributes to the effectiveness of its information security program. The information security program is more effective when security processes are deeply embedded in the institution's culture and there is a high level of **security awareness**. The management team should understand and support information security and provide appropriate resources for developing, implementing, and maintaining the information security program. The result of this understanding and support is a program in which both management and employees are committed to integrating the program into lines of business, support functions, and third-party management programs.¹

4.1 The Basics of Security for Social Engineering Attacks

Protection against social engineering attacks and other **security threats** is essential for all organizations. Attackers use malware to obtain access to an organization's network and computer environment and to execute an attack within the environment. Malware may enter through public or private networks and from devices attached to the network. Although protective mechanisms may block most malware before they do any damage, even a single malicious executable file may create a significant potential for loss.

The implementation of an in-depth defensive program to protect, detect, and respond to malware is an important basic step. Businesses can use many tools to block malware before it enters the network and

to detect it and respond if it is not blocked. Methods or systems that management should consider include the following:

- Hardware-based roots of trust, which use cryptographic means to verify the integrity of software.
- Servers that run active content at the gateway and disallow content based on policy.
- Blacklists that disallow code execution based on code fragments, Internet locations, and other factors that correlate with malicious code.
- White lists of allowed programs.
- Port monitoring to identify unauthorized network connections.
- Network segregation.
- Computer configuration to permit the least amount of privileges necessary to perform the user's job.
- Application **sandboxing**.
- Monitoring for unauthorized software and disallowing the ability to install unauthorized software.
- Monitoring for anomalous activity for malware and polymorphic code.
- Monitoring of network traffic.
- User education in awareness, **security vigilance**, safe computing practices, indicators of malicious code, and response actions.²

Training is absolutely essential for security against social engineering and malicious code attacks, but it is neglected by far too many organizations. Training ensures personnel have the necessary knowledge and skills to perform their job functions. Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Organizations should educate users about their security roles and responsibilities and communicate them through acceptable use policies. Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and

other assets are protected. Management should also have the ability to impose sanctions for noncompliance.

Training materials for most users focus on issues such as endpoint security, login requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through email or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. Management should collect signed acknowledgments of the employee **acceptable use policy** as part of the annual training program.³

Acceptable use policies should emphasize that an organization's computer and networks will not be used for personal activities. This is a very important principle. Employee's **personal use** expands the profile of a network and domain and can open the environment to a larger number of social engineering attacks and malware infestations. Employees may feel this is harsh but the goal of a security plan and security policy is to protect the networks and electronic assets so that operations are not disrupted.

4.2 Applying the Cybersecurity Framework is an Ongoing Process

Recognizing that national and economic security of the United States depends on the reliable functioning of critical infrastructure, the president issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The Order directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. The Cybersecurity Enhancement Act of 2014 reinforced NIST's EO 13636 role.

Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. The Cybersecurity Framework consists of three main components: the Core, Implementation Tiers, and Profiles.

The Framework Core provides a set of desired cybersecurity activities and outcomes using common language that is easy to understand. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.

The Framework Implementation Tiers assist organizations by providing context for an organization to view cybersecurity risk management. The Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget.

Framework Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.⁴

The Framework will help an organization better understand, manage, and reduce its cybersecurity risks. It will assist in determining which activities are most important to assure critical operations and service delivery. In turn, that will help prioritize investments and maximize the impact of each dollar spent on cybersecurity. By providing a common language to address cybersecurity risk management, it is especially helpful in communicating inside and outside the organization. That includes improving communication, awareness, and understanding between and among information technology (IT), planning, and operating units, as well as senior executives of organizations. Organizations can also readily use the Framework to communicate current or desired cybersecurity posture between a buyer and supplier.

The Framework is guidance. It should be customized by different sectors and individual organizations to best suit their risks, situations, and needs. Organizations will continue to have unique risks as they face different threats and have different vulnerabilities and risk tolerances, and how they implement the practices in the Framework to achieve positive outcomes will vary. The Framework should not be implemented using a one-size-fits-all approach for critical infrastructure organizations or as an un-customized checklist.

Organizations are using the Framework in a variety of ways. Many have found it helpful in raising awareness and communicating with stakeholders within their organizations, including the executive

BOX 4.1 HIGH PRIORITY AREAS FOR DEVELOPMENT IN THE CYBERSECURITY FRAMEWORK

Authentication
Automated indicator sharing
Conformity assessment
Cybersecurity workforce
Data analytics
Federal agency cybersecurity alignment
International aspects, impacts, and alignment
Supply chain risk management
Technical privacy standards

leadership. The Framework is also improving communication across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. By mapping the Framework to current cybersecurity management approaches, organizations are learning and showing how they match up with the Framework's standards, guidelines, and best practices. Some parties are using the Framework to reconcile and de-conflict internal policy with legislation, regulation, and industry best practice. The Framework is also being used as a strategic planning tool to assess risks and current practices.

The Framework can be used by organizations that already have extensive cybersecurity programs, as well as by those just beginning to think about putting cybersecurity management programs in place. The same general approach works for any organization, although the way in which they make use of the Framework will differ depending on their current state and priorities. The high-priority areas for the development of practices, standards, and technologies necessary to support the Framework are shown in Box 4.1.⁵

4.3 The Framework Components

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. An example of Framework outcome

language is physical devices and systems within the organization are inventoried.

The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions, which are shown in Box 4.2. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function and matches them with example Informative References, such as existing standards, guidelines, and practices for each Subcategory.

A Framework Profile represents the cybersecurity outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing an as is security condition to a desired security condition. To develop a Profile, an organization can review all the Categories and Subcategories and, based on business drivers and a risk assessment, determine which ones are most important for them. They can also add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to

BOX 4.2 THE FRAMEWORK CORE: CONCURRENT AND CONTINUOUS FUNCTIONS

Identify
Protect
Detect
Respond
Recover

conduct self-assessments and communicate within an organization or between organizations.

Framework Implementation Tiers provide the context for how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

The Framework Implementation Tiers are not intended to be maturity levels. The Tiers are intended to provide guidance to organizations on the interactions and coordination between cybersecurity risk management and operational risk management. The key tenet of the Tiers is to allow organizations to take stock of their current activities from an organization-wide point of view and determine if the current integration of cybersecurity risk management practices is sufficient, given their mission, regulatory requirements, and risk appetite. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and would be cost-effective.

The companion Roadmap was initially released in February 2014 in unison with the publication of the Framework version 1.0. The Roadmap discusses NIST's next steps with the Framework and identifies key areas of development, alignment, and collaboration. These plans are based on input and feedback received from stakeholders through the Framework development process. This list of high-priority areas is not intended to be exhaustive, but these are important areas identified by NIST and stakeholders that should inform future versions of the Framework. For that reason, the Roadmap will be updated over time in alignment with the most impactful stakeholder cybersecurity activities and the Framework itself.

Each organization's cybersecurity resources, capabilities, and needs are different. So the time to implement the Framework will vary among organizations, ranging from as short as a few weeks to several

years. The Framework Core's hierarchical design enables organizations to apportion steps between current state and desired state in a way that is appropriate to their resources, capabilities, and needs. This allows organizations to develop a realistic action plan to achieve Framework outcomes in a reasonable time frame, and then build upon that success in subsequent activities.

The Framework provides guidance relevant to the entire organization. The full benefits of the Framework will not be realized if only the IT department uses it. The Framework balances comprehensive risk management, with a language that is adaptable to the audience at hand. More specifically, the Function, Category, and Subcategory levels of the Framework correspond well to organizational, mission/business, and IT and operational technology (OT)/industrial control system (ICS) professionals at the systems level. This enables accurate and meaningful communication from the C-suite to individual operating units and with supply chain partners. It can be especially helpful in improving communications and understanding between IT specialists, OT/ICS operators, and senior managers of the organization.⁶ The complete Cybersecurity Framework can be found at www.nist.gov/cyberframework.

4.4 Developing Security Policies

While policies themselves do not solve problems, and in fact can actually complicate things unless they are clearly written and observed, they do define the ideal toward which all organizational efforts should point. By definition, security policy refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it. A good policy protects not only information and systems, but also individual employees and the organization as a whole. It also serves as a prominent statement to the outside world about the organization's commitment to security.

Tenable security policy must be based on the results of a risk assessment. Findings from a risk assessment provide policymakers with an accurate picture of the security needs specific to their organization. Risk assessments also help expose **gaps in security**, which is imperative for proper policy development, something that requires several steps on the part of decision-makers as are shown in Box 4.3.

BOX 4.3 STEPS DECISION-MAKERS MUST TAKE TO DEVELOP SECURITY POLICIES

- Identify sensitive information and critical systems
- Incorporate local, state, and federal laws, as well as relevant ethical standards
- Define institutional security goals and objectives
- Set a course for accomplishing those goals and objectives
- Ensure that necessary mechanisms for accomplishing the goals and objectives are in place

Although finalizing organizational policy is usually a task reserved for top-level decision-makers, contributing to the development of policy should be an organization-wide activity. While every employee doesn't necessarily need to attend each security policy planning session, top-level managers should include representatives from all job levels and types in the information gathering phase (just as in the case of brainstorming during risk assessment). Non-administrative employees have an especially unique perspective to share with policy-makers that simply cannot be acquired by any other means. Meeting with staff on a frequent basis to learn about significant issues that affect their work is a big step toward ensuring that there is buy-in at all levels of the organization.

It was pointed out in previous chapters that all organizations are vulnerable to social engineering attacks and indeed organizations from all sectors have been impacted by such attacks. Although an organization's risk assessment informs managers of their system's specific security needs, in the case of social engineering attacks all types and sizes of organizations need to take steps to mitigate such attacks. Regardless of any findings from a risk assessment, the following general questions should be addressed clearly and concisely in any security policy:

- What is the reason for the policy?
- Who developed the policy?
- Who approved the policy?
- Whose authority sustains the policy?
- Which laws or regulations, if any, are the policies based on?

- Who will enforce the policy?
- How will the policy be enforced?
- Whom does the policy affect?
- What assets must be protected?
- What are users actually required to do?
- How should security breaches and violations be reported?
- What are the effective date and expiration date of the policy?

Policies should be written in plain language and understandable to their intended audience. They should be concise and focus on expectations and consequences, but it is helpful to explain why the policies are being put into place. In addition, any term that could potentially confuse a reader needs to be defined. By keeping things as simple as possible, employee participation becomes a realistic aspiration. But bear in mind that unless the organization educates its users, there is little reason to expect security procedures to be implemented properly.

Employee training that is specifically tailored to meet the requirements of the security policy should be implemented. Policy makers should recognize that many computer users may not be trained to use technology properly and what little training they have had was probably aimed at overcoming their fears and teaching them how to turn on their machines. At most, they may have learned how to use a particular piece of software for a specific application. Thus, the majority of an organization's employees would have little understanding of security issues, and there would be no reason to expect that to change unless the organization does its part to correct the situation and provide appropriate training. Reluctance on the part of the organization to adequately prepare employees for making security policy a part of the work environment makes the rest of the effort an exercise in the theoretical—and theory will not protect a system from threats that are all too real.

Expecting every employee to become a security expert is wholly unrealistic. Instead, recommended security practices should be broken down into manageable pieces that are tailored to meet individual job duties. A single, short, and well-focused message each week will be better received than a monthly volume of information that is overly ambitious.

Without proof that an employee agreed to abide by security regulations, the sometimes necessary tasks of reprimanding, dismissing, or

even prosecuting security violators can be difficult to pursue. One aim of a successful security policy is that it should limit the need for trust in the system. While this may seem like a terribly cynical philosophy, it actually serves to protect both the organization's employees and the organization itself. But before the benefits of security can be realized, staff must be properly informed of their roles, responsibilities, and organizational expectations. Employees must be told in writing including what is and is not acceptable use of equipment and that security will be a part of performance reviews.

Whenever security is threatened, whether it is a disk crash, an external intruder attack, or a natural disaster, it is important to have planned for the potential adverse events in advance. The only way to be sure that you have planned in advance for such troubles is to plan now, because you can never predict exactly when a security breach will happen. It could happen in a year, a month, or this afternoon. Planning for emergencies beforehand goes beyond good policy. There is no substitute for security breach response planning and other overarching contingency planning.⁷

4.5 Protecting Small Businesses from Social Engineering Attacks

There are numerous opportunities for small businesses to fill needed niches in industry or business services. Broadband and information technology are powerful factors in small businesses reaching new markets and increasing productivity and efficiency. However, many small businesses may not have all the resources they need to have a strong cybersecurity posture but they still need a cybersecurity strategy to protect their own business, their customers, and their data from growing cybersecurity threats. The Federal Communications Commission (FCC), the Department of Homeland Security (DHS), and the Small Business Administration have all provided advice for small businesses.

The 30 million small businesses in the United States create about two out of every three new jobs in the US each year, and more than half of Americans either own or work for a small business. Small businesses play a key role in the economy and in the nation's supply chain, and they are increasingly reliant on information technology to store, process, and communicate information. Protecting this information against increasing cyber threats is critical.

Small employers often do not consider themselves targets for cyber attacks due to their size or the perception that they don't have anything worth stealing. However, small businesses have valuable information cybercriminals seek, including employee and customer data, bank account information and access to the business's finances, and intellectual property. Small employers also provide access to larger networks such as supply chains.

While some small employers already have robust cybersecurity practices in place, many small firms lack sufficient resources or personnel to dedicate to cybersecurity. Given their role in the nation's supply chain and economy, combined with fewer resources than their larger counterparts to secure their information, systems, and networks, small employers are an attractive target for cybercriminals.⁸

The National Cybersecurity and Communications Integration Center (NCCIC) received multiple reports of WannaCry ransomware infections worldwide. Ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered through social engineering attacks and phishing emails, and it exploits unpatched vulnerabilities in software. Phishing emails are crafted to appear as though they have been sent from a legitimate organization or known individual. These emails often entice users to click on a link or open an attachment containing malicious code. After the code is run, a computer may become infected with malware.

A commitment to cyber hygiene and **best practices** is critical to protecting organizations and users from cyber threats, including malware. In advice specific to the recent social engineering attacks and WannaCry ransomware threat, users should:

- Be careful when clicking directly on links in emails, even if the sender appears to be known; attempt to verify web addresses independently (e.g., contact the organization's help desk or search the Internet for the main website of the organization or topic mentioned in the email).
- Exercise caution when opening email attachments. Be particularly wary of compressed or ZIP file attachments.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other

internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

- Avoid providing personal information or information about the organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Avoid revealing personal or financial information in emails, and do not respond to email solicitations for this information. This includes following links sent in emails.
- Be cautious about sending sensitive information over the Internet before checking a website's security.⁹

If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use the contact information provided on a website connected to the request; instead, check previous statements for contact information. Small businesses should also do the following:

- Train employees in security principles and establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies.
- Protect information, computers, and networks from cyber attacks by keeping clean machines: Having the latest security software, web browser, and operating systems are the best defenses against viruses, malware, and other online threats. Set anti-virus software to run a scan after each update. Install other key software updates as soon as they are available.
- Provide firewall security for the Internet connection and make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.
- Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password-protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information

while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

- Regularly back up the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Back up data automatically if possible, or at least weekly and store the copies either off-site or in the cloud.
- Prevent access to or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.
- Ensure that the Wi-Fi network for the workplace is secure, encrypted, and hidden. To hide the Wi-Fi network, the wireless access point or router should be set up such that it does not broadcast the network name, known as the Service Set Identifier (SSID). Also, access to the router should be password protected.
- Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. Companies may also have additional security obligations pursuant to agreements with their bank or processor. They should ensure that payment systems are isolated from other, less secure programs and that the same computer is not used to process payments and surf the Internet.
- Ensure that no one employee is provided with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.
- Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.¹⁰

- Make sure each of your business's computers is equipped with anti-virus software and anti-spyware, and updated regularly. Such software is readily available online from a variety of vendors. All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install updates automatically.
- Educate employees about online threats and how to protect the business's data, including the safe use of social networking sites. Depending on the nature of the business, employees might be introducing competitors to sensitive details about the firm's internal business via social networking sites. Employees should be informed about how to post online in a way that does not reveal any trade secrets to the public or competing businesses.
- Protect all pages on public-facing websites, not just the check-out and sign-up pages.¹¹

4.6 Establishing a Culture of Security

When managing a network, developing an app, or even organizing paper files, sound security is no accident. Companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved. Threats to data may transform over time, but the fundamentals of sound security remain constant.

From personal data on employment applications to network files with customers' credit card numbers, sensitive information pervades every part of many companies. Business executives often ask how to manage confidential information. The key first step is to start with security. Factor it into the decision-making in every department of the organization including personnel, sales, accounting, information technology. Collecting and maintaining information just because it can be collected is no longer a sound business strategy. Savvy companies think through the implications of their data decisions. Making conscious choices about the kind of information to collect, how long to keep it, and who can access it, can reduce the risk of a data compromise

down the road. Of course, all of those decisions will depend on the nature of the business.

Sometimes it's necessary to collect personal data as part of a transaction. But once the deal is done, it may be unwise to keep it. In the Federal Trade Commission's (FTC's) BJ's Wholesale Club case, the company collected customers' credit and debit card information to process transactions in its retail stores. But according to the complaint, it continued to store that data for up to 30 days, long after the sale was complete. Not only did that violate bank rules but, by holding on to the information without a legitimate business need, the FTC said BJ's Wholesale Club created an unreasonable risk. By exploiting other weaknesses in the company's security practices, hackers stole the account data and used it to make counterfeit credit and debit cards. The business could have limited its risk by securely disposing of the financial information once it no longer had a legitimate need for it.

If employees do not have to use personal information as part of their job, there is no need for them to have access to it. For example, in the Goal Financial case, the FTC alleged that the company failed to restrict employee access to personal information stored in paper files and on its network. As a result, a group of employees transferred more than 7,000 consumer files containing sensitive information to third parties without authorization. The company could have prevented that misstep by implementing proper controls and ensuring that only authorized employees with a business need had access to people's personal information.

Passwords like 121212 or qwerty are not much better than no password at all. That's why it's wise to give some thought to the password standards you implement. In the Twitter case, for example, the company let employees use common dictionary words as administrative passwords, as well as passwords they were already using for other accounts. According to the FTC, those lax practices left Twitter's system vulnerable to hackers who used password-guessing tools or tried passwords stolen from other services in the hope that Twitter employees used the same password to access the company's system. Twitter could have limited those risks by implementing a more secure password system, for example, by requiring employees to choose complex passwords and training them not to use the same or similar passwords for both business and personal accounts.

In the Guidance Software case, the FTC alleged that the company stored network user credentials in clear, readable text that helped a hacker gain access to customer credit card information on the network. Similarly, in the Reed Elsevier case, the FTC charged that the business allowed customers to store user credentials in a vulnerable format in cookies on their computers. In Twitter, too, the FTC said the company failed to establish policies that prohibited employees from storing administrative passwords in plain text in personal email accounts. In each of those cases, the risks could have been reduced if the companies had policies and procedures in place to store credentials securely.

In the Lookout Services case, the FTC charged that the company failed to adequately test its web application for widely known security flaws, including one called predictable resource location. As a result, a hacker could easily predict patterns and manipulate URLs to bypass the web app's authentication screen and gain unauthorized access to the company's databases. The company could have improved the security of its authentication mechanism by testing for common vulnerabilities.

Data does not stay in one place. That's why it's important to consider security at all stages if transmitting information is a necessity for your business. In the Superior Mortgage Corporation case, for example, the FTC alleged that the company used Secure Sockets Layer (SSL) encryption to secure the transmission of sensitive personal information between the customer's web browser and the business's website server. But once the information reached the server, the company's service provider decrypted it and emailed it in clear, readable text to the company's headquarters and branch offices. That risk could have been prevented by ensuring the data was secure throughout its lifecycle and not just during the initial transmission.

The FTC's actions against Fandango and Credit Karma alleged that the companies used SSL encryption in their mobile apps, but turned off a critical process known as SSL certificate validation without implementing other compensating security measures. That made the apps vulnerable to man-in-the-middle attacks, which could allow hackers to decrypt sensitive information the apps transmitted. Those risks could have been prevented if the companies' implementations of SSL had been properly configured.

In the Dave & Buster's case, the FTC alleged that the company did not use an intrusion detection system and did not monitor system logs for suspicious activity. The FTC said something similar happened in the Cardsystem Solutions case. The business did not use sufficient measures to detect unauthorized access to its network. Hackers exploited weaknesses, installing programs on the company's network, which collected stored sensitive data and sent it outside the network every four days. In each of these cases, the businesses could have reduced the risk of a data compromise, or the breadth of that compromise, by using tools to monitor activity on their networks.

In cases like MTS, HTC America, and TRENDnet, the FTC alleged that the companies failed to train their employees in secure coding practices. The upshot: Questionable design decisions, including the introduction of vulnerabilities into the software. For example, according to the complaint in HTC America, the company failed to implement readily available secure communication mechanisms in the logging applications it pre-installed on its mobile devices. As a result, malicious third-party apps could communicate with the logging applications, placing consumers' text messages, location data, and other sensitive information at risk. The company could have reduced the risk of vulnerabilities like that by adequately training its engineers in secure coding practices.

Security cannot be a take-our-word-for-it thing. Including security expectations in contracts with service providers is an important first step, but it is also important to build oversight into the process. The FTC Upromise case illustrates that point. There, the company hired a service provider to develop a browser toolbar. Upromise claimed that the toolbar, which collected consumers' browsing information to provide personalized offers, would use a filter to remove any personally identifiable information before transmission. But, according to the FTC, Upromise failed to verify that the service provider had implemented the information collection program in a manner consistent with Upromise's privacy and security policies and with the terms in the contract designed to protect consumer information. As a result, the toolbar collected sensitive personal information—including financial account numbers and security codes from secure web pages—and transmitted it in clear text. How could the company have reduced that risk? By asking questions and following up with the service provider during the development process.¹²

Responding to the dramatic changes in computing power, use of the Internet, and development of networked systems, the Organization of Economic Cooperation and Development (OECD) guidelines provide a set of principles to help ensure the security of contemporary interconnected communication systems and networks. They are applicable to all, from those who manufacture, own, and operate information systems to those individual users who connect through home PCs. Importantly, the guidelines call for new ways of thinking and behaving when using information systems. They encourage the development of a **culture of security** as a mindset to respond to the threats and vulnerabilities of communication networks. The nine principles address: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. The guidelines were developed with the full cooperation of the OECD's Business Industry Advisory Council (BIAC) and representatives of civil society.

In October 2001, the OECD Committee on Information, Computer, and Communication Policy (ICCP) responded positively to a US proposal for an expedited review of the security guidelines. The OECD member countries, businesses, civil society, and the OECD Secretariat shared a sense of urgency and responded with full cooperation and support. The text of the guidelines is available at www.oecd.org.

Completion of the guidelines is only the first step. US government agencies used the guidelines in their outreach activities to the private sector, the public, and other governments and encouraged business, industry, and consumer groups to join in using the guidelines as they developed their own approaches to the security of information systems and networks, and in the development of a culture of security for information systems and networks.¹³

4.7 Conclusion

Defending against social engineering attacks is a necessity for all types and sizes of organizations. The information security program is more effective when security processes are deeply embedded in the institution's culture. Effective security must be a substantive part of organization culture and training must occur on an ongoing basis.

4.8 Key Points

Important points presented in this chapter are as follows:

- Training is absolutely essential to security against social engineering and malicious code attacks but it is neglected by far too many organizations.
- The Cybersecurity Framework consists of three main components: The Core, Implementation Tiers, and Profiles. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity in an organization.
- The Framework is guidance. It should be customized by different sectors and individual organizations to best suit their risks, situations, and needs. Organizations will continue to have unique risks, face different threats, and have different vulnerabilities and risk tolerances. How they implement the practices in the Framework to achieve positive outcomes will vary.
- The term security policy refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it.
- Policies should be concise and focus on expectations and consequences, but it is helpful to explain why the policies are being put into place.
- Many small businesses may not have all the resources they need to have a strong cybersecurity posture. However, businesses need a cybersecurity strategy to protect their own organization, customers, and data from growing cybersecurity threats.
- Companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved.
- Making conscious choices about the kind of information to collect, how long to keep it, and who can access it, can reduce the risk of a data compromise down the road.
- The Organization of Economic Cooperation and Development (OECD) guidelines encourage the development of a culture of security as a mindset to respond to the threats and vulnerabilities of communication networks.

4.9 Seminar Discussion Topics

Discussion topics for graduate- or professional-level seminars are:

- What experience have seminar participants had in assessing the state of security in an organization? What were the results of those assessments?
- What experience have seminar participants had in developing security policies for an organization? What type of policies did they develop?
- What experience have seminar participants had in reassessing security practices and policies after a security breach occurred in an organization? What were the results of the reassessment?

4.10 Seminar Group Project

Participants should interview people from five different organizations to determine what the interviewees understand about cybersecurity in their organizations. They should then write up a one-page summary of each interview and share them in a discussion group in the seminar.

Key Terms

Acceptable use policy: is a document that establishes an agreement between users and the enterprise and defines for all parties the ranges of use that are approved before users can gain access to a network or the Internet.

Best practices: are techniques or methodologies that, through experience and research, have reliably led to a desired or optimum result.

Culture of security: is an organization culture in which security pervades every aspect of daily life as well as all in all operational situations.

Gaps in security: are security measures or mitigation methods that are inadequate to protect an asset or do not thoroughly protect the asset that they were deployed to protect.

Personal use: means using a service or an item for personal reasons and goals that do not have any relationship to the organization employing the individual using the item or service.

Sandboxing: is the use of a restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized to limit the access and functionality of the executed code.

Security awareness: is the basic level of understanding of security and recognition of the importance of security.

Security threats: are conditions, people, or events that can jeopardize the security of a nation, organization, a facility, or any asset belonging to the threatened entity.

Security vigilance: is a constant attention given to security during day-to-day operations; it contributes to security by encouraging the reporting of security violations, and it makes suggestions on how to improve security when weaknesses are observed.

References

1. Security Culture. Federal Financial Institutions Examination Council. Accessed February 10, 2019. <https://ithandbook.ffiec.gov/it-booklets/information-security/i-governance-of-the-information-security-program/ia-security-culture.aspx>
2. Malware Mitigation. Federal Financial Institutions Examination Council. Accessed February 10, 2019. <https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic12-malware-mitigation.aspx>
3. Training. Federal Financial Institutions Examination Council. Accessed February 10, 2019. [https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7\(e\)-training.aspx](https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7(e)-training.aspx)
4. New to Framework. NIST. December 11, 2018. Accessed February 10, 2019. <https://www.nist.gov/cyberframework/new-framework#background>
5. Framework Basics. NIST. December 11, 2018. Accessed February 10, 2019. <https://www.nist.gov/cyberframework/questions-and-answers#framework>
6. Framework Components. NIST. December 11, 2018. Accessed February 10, 2019. <https://www.nist.gov/cyberframework/questions-and-answers#framework>
7. Security Policy: Development and Implementation. US Department of Education, the Institute of Education Sciences (IES). Accessed February 10, 2019. <https://nces.ed.gov/pubs98/safetech/chapter3.asp>

8. Introduction to Cybersecurity. US Small Business Administration. Accessed February 10, 2019. <https://www.sba.gov/managing-business/cybersecurity/introduction-cybersecurity>
9. Protect Against Ransomware. US Small Business Administration. Accessed February 10, 2019. <https://www.sba.gov/managing-business/cybersecurity/protect-against-ransomware>
10. Cybersecurity for Small Business. US Federal Communications Commission. Accessed February 10, 2019. <https://www.fcc.gov/general/cybersecurity-small-business>
11. Top Ten Cybersecurity Tips. US Small Business Administration. Accessed February 10, 2019. <https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips>
12. Start with Security: A Guide for Business. FTC. June 2005. Accessed February 11, 2019. <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business#start>
13. OECD Calls for Culture of Security for Information Systems. Organization of Economic Cooperation and Development (OECD). August 2002. Accessed February 11, 2019. <https://2001-2009.state.gov/r/pa/prs/ps/2002/12518.htm>



CHAPTER

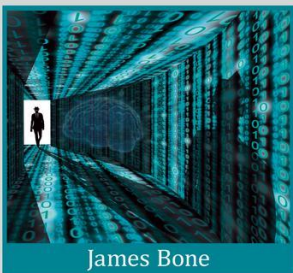
2

COGNITIVE BEHAVIOR

INTERNAL AUDIT AND IT AUDIT SERIES

Cognitive Hack

The New Battleground in
Cybersecurity... the Human Mind



James Bone

 CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

This chapter is excerpted from

Cognitive Hack

The New Battleground in Cybersecurity ... the Human Mind

by James Bone

© [2017] Taylor & Francis Group. All rights reserved.



[Learn more](#)

COGNITIVE BEHAVIOR

Advances in Situational Awareness

Only amateurs attack machines; professionals target people.

Bruce Schneier (2000)

Just as military battles are no longer fought in trenches, with massive armored vehicles clashing in open fields, cyberwars are transforming the battlespace of the future.* In military parlance, the introduction of urban fighters and mobile targets changed how proxy wars are fought. Asymmetric in execution, military leaders had to adapt to unconventional tactics in response to new threats. Cyber risk is also three dimensional in a digital sense. The first dimension is advanced technology, followed by cognitive hacks, with the end result being real collateral damage in time, expense, and reputation.

In Chapter 1, we discussed the inherent weakness in building “Maginot Lines” to defend the fort with layers upon layers of security protocols that have proven ineffective in preventing attack. The question remains: If not some form of Maginot Lines, what has proven more effective? I explore that question by summarizing research findings and asking more questions that remain unanswered. However, as the costs to defend and mitigate attacks escalate, senior management will demand ways to slow or lower the cost of cybersecurity.

How will security professionals respond? What new approaches are available to improve security and lower the cost of defending the fortress? Firms must consider new ways to address the asymmetric nature of cyberattacks using their own toolkit of asymmetric defenses. One such set of new tools being explored by the military, government agencies, and a host of industries is the domain of human behavior and cognitive sciences.

* <http://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare>

A subset of these disciplines includes Cyber Situational Awareness, Cyber Hacking and Intelligence and Security Informatics, Cognitive Hacking, Ontology Mapping, Semantic Architecture, Prospect Theory–Cognitive Bias and Heuristics, and others. Each of these areas reflects exhaustive scientific research beyond the scope of this book but deserves a mention to demonstrate the progress made to date. Much of the new research in cybersecurity is in the early stage of development and no one subject should be considered a panacea as a whole.

One thing that is becoming clear is that human behavior and cognition will play a central role in advancing the practice of cybersecurity. I would not do justice to cover each of these disciplines in-depth at this time, nor was it the intention to do so. The goal of *Cognitive Hack* is to introduce readers to the evolution of emerging technologies, many in very early stage of development, being considered to address what some believe to be the weakest link in cybersecurity—the human mind. The remainder of the book will expand on cognitive hacking and other semantic attacks.

The additional disciplinary topics should be covered separately as an in-depth analysis to expand the understanding of how these technologies will be arrayed in combating cyber risks. Cognitive hacking and semantic attacks are currently two of the most commonly used tools of the hacker trade but by no means the only tools. The goal then is to make readers aware of emerging new disciplines in cybersecurity with the understanding that the field is very wide in topical research but somewhat shallow in application at this time.

It is also important to point out that each of these topics requires singular attention to understand them fully. It is my intention to introduce readers to a more thorough analysis of these disciplines as the opportunity presents itself and desire is demonstrated for more details. The goal here is to demonstrate how security is evolving and to develop a process for governance and a framework for operationalizing a cognitive risk program inclusive of advanced technologies as they emerge and practical steps for understanding risk beyond today's simplistic and qualitative approach to risk assessment. I may, at times, use the terms cognitive hack and semantic attack interchangeably. The distinctions are slight, with cognitive hack referencing a broader range of tactics used by hackers to change or trick the user's behavior

and semantic attacks to depict the use of written text and a range of deceptive communications to accomplish the same goal.

Cyber situational awareness is the hottest new buzzword in cybersecurity and the subject of new research on the role cognition contributes, negatively or positively, to cybersecurity. Although the term situational awareness is an old concept to describe something we do instinctually, nonetheless there are subtleties embedded in the definition that are unique to cybersecurity.

What is situational awareness? Situation awareness is defined as “the perception of environmental elements with respect to time or space, the comprehension of their meaning, and the projection of their status after some variable has changed, such as time, or some other variable, such as a predetermined event.”* “It is also a field of study concerned with understanding the environment critical to decision makers in complex, dynamic areas from aviation, air traffic control, ship navigation, power plant operations, military command and control, and emergency services such as firefighting and policing to more ordinary but nevertheless complex tasks such as driving an automobile or riding a bicycle.”* The National Institute of Standards and Technology (NIST), an internationally accepted standard on IT security, has also advocated for and developed a framework of continuous monitoring to provide security analysts with situational awareness. See Figure 2.1.

Situational awareness is not a new concept, “the concept has roots in the history of military theory[†]—it is recognizable in Sun Tzu’s *The Art of War*,”[‡] for instance. The term itself can be traced also to World War I,[§] “where it was recognized as a crucial component for crews in military aircraft.” The term was first used in the 1990s by the U.S. Air Force; its pilots returning from successfully runs attributed their success to having good situational awareness over their opponents. Pilots suggested their survival in dogfights typically amounted to observing the opponent and reacting within seconds before the other pilot anticipated their own action. Col. John Boyd, ace USAF pilot

* https://en.wikipedia.org/wiki/Situation_awareness

† https://en.wikipedia.org/wiki/Military_theory

‡ https://en.wikipedia.org/wiki/The_Art_of_War

§ https://en.wikipedia.org/wiki/World_War_I

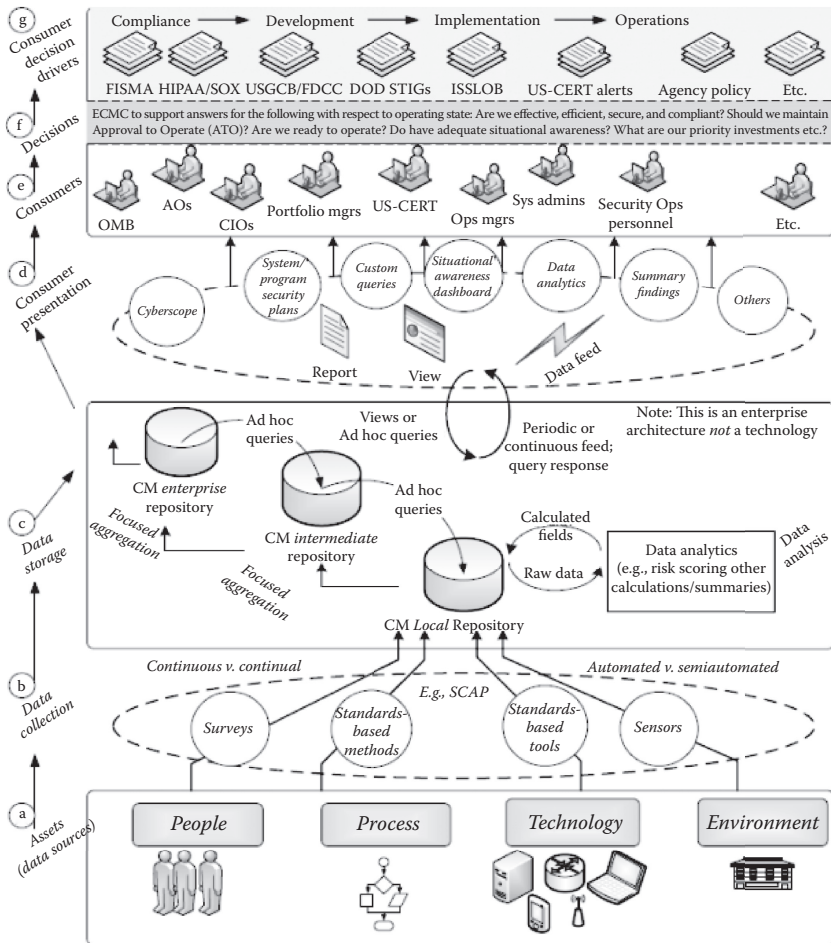


Figure 2.1 Diagram of the elements of “Continuous Monitoring” in the NIST IR 7756 draft.

and war theorist, described the “observe” and “orient” part of situational awareness as a factor in the development of the Boyd Loop or Observe-Orient-Decide-Act Loop. If a pilot lost situational awareness in battle, he was considered “out of the loop.”

“It is important to distinguish the term situation awareness (Endsley, 1988a,b), as a state of knowledge, from the processes used to achieve that state.* These processes, which may vary widely among individuals and contexts, will be referred to as situational assessment or the process of achieving, acquiring, or maintaining SA.” Thus, in

* https://en.wikipedia.org/wiki/Situation_awareness#cite_note-20

brief, *situational awareness* is viewed as “a state of knowledge,” and *situational assessment* as “the processes” used to achieve that knowledge. Note that the processes of situational assessment not only produce situational awareness, but they also drive those same processes in a recurrent fashion. For example, one’s current awareness can determine what one pays attention to next and how one interprets the information perceived (Endsley, 1988a,b). Situational Awareness Global Assessment Technique (SAGAT).*

Situational awareness is a mental model for sensemaking under uncertain conditions but how does one operationalize situational awareness? “Situation awareness is about the knowledge state that’s achieved—either knowledge of current data elements, or inferences drawn from these data, or predictions that can be made using these inferences. In contrast, sensemaking is about the process of achieving these kinds of outcomes, the strategies, and the barriers encountered.”†

To understand better what this means we need to break the definition down into simpler terms. MITRE, a government contract vendor who specializes in cybersecurity, describes the processes involved in cyber situational awareness as a framework. “Comprehensive cyber situation awareness involves three key areas: computing and network components, threat information, and mission dependencies.” Put more simply, business and government leaders must anticipate what might happen to their systems and develop effective countermeasures to protect their mission-critical applications.

If this sounds like common sense masquerading as “consultant-speak” you would not be alone in thinking it’s another fad destined for the dustbin of good intentions. But before you dismiss this concept out of hand, I would ask that you suspend disbelief for now and consider the data we have covered so far. No doubt you personally have experience with clicking on a link with a virus or had to mitigate a security exposure due to poor judgment by yourself or a colleague.

Situational awareness is the basis for automating analytical models in cybersecurity programs to anticipate and address cyberattacks more effectively. Situational awareness provides a framework for recognizing when the environment deviates from expectations and formulates

* <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=195097>

† https://en.wikipedia.org/wiki/Situation_awareness#cite_note-28

a set of actions to be taken in response to a perceived threat or change in dynamics.

“A loss of situational awareness has been identified as a root cause for human errors in judgment or delayed response to threats in the theater of operation.” Behavioral economists, research psychologists, and other scientists have helped to shed light on how simple it is to lose sight of situational awareness. Daniel Kahneman and Amos Tversky’s Prospect theory is now widely accepted reading for understanding decision making under uncertain conditions. Prospect theory helps explain the mental mechanics for how and why we are more prone to make mistakes of judgment when faced with incomplete information.

Kahneman and Tversky (2000) described their original theory as being “concerned with the behavior of decision makers who face a choice between two alternatives.” The definition in the original text is: “Decision making under risk can be viewed as a choice between prospects or gambles.” Decisions subject to risk are deemed to signify a choice between alternative actions, which are associated with particular probabilities (prospects) or gambles.” What Kahneman and Tversky learned is that we lack the tools to choose consistently among options involving probability when the outcomes are less certain (Goldberg and von Nitzsch, 2001, p. 62). Prospect theory provides a broader framework for understanding cognitive bias and heuristics as well as how uncertainty leads us astray.

Think of situational awareness as the techniques to *not* send an invitation that prompts an attack but, if attacked, to initiate robust countermeasures in response. Why phrase it this way? “Libicki first characterized attacks on computer systems in the context of information warfare as being physical, syntactic, and semantic, where software agents were misled by misinformation deliberately fed by an adversary.”*†

The framework for situational awareness is a fusion of concepts borrowed from war theorists from the navy and air force. Officers from the U.S. Air Force are credited with developing the “Observe–Orient–Decide–Act” Loop (OODA Loop). The OODA Loop formally defined the foundational processes for situation awareness required in successful aerial combat missions. OODA has since been

* <http://www.ists.dartmouth.edu/library/77.pdf> reference for Libicki quote

† <https://www.schneier.com/crypto-gram/archives/2000/1015.html>

refined into a more elaborate framework for situational awareness over time as more sophisticated applications have evolved. The cognitive processes involved in situational awareness are situational understanding, situational assessment, mental models, and sensemaking. It's important to unpack each process to clarify how the integration of each step leads to effective situational awareness.

Situational understanding is the “so what” of the cumulative data and information gathering applied to the analysis and judgment of observations in the operational theater. Situational understanding encompasses the first step, “Observe,” in the OODA Loop. *Situational assessment* represents the “Orient” processes used to gain knowledge about the environment. These processes may be quantitative and/or qualitative and include data from external sources to supplement or fill in gaps in knowledge.

Situational assessment is used to build mental models representing experiential learning, expertise, and intuition used to assess the environment and make an appropriate selection among possible scenarios presented in the theater. *Mental models* represent the next step, “Decide,” in the OODA Loop.

Mental models create a set of behavioral responses to the possible scenarios observed. The purpose of a formalized mental model is to shorten the reaction time in various threat scenarios while reducing the possibility of judgment error.

Finally, *sensemaking* is the process of identifying patterns in the data or knowledge gathered to choose an appropriate course of actions. Sensemaking represents the final step, “Act,” in the OODA Loop and serves to confirm the response decision. The OODA Loop is not static. Depending on the complexity of the situation, several rounds of analysis may be required to come to a reasonable conclusion.

What are the practical applications of situational awareness in cybersecurity? One way to better understand a real-time example of situational awareness is to look at the backstory of the cyberattack on Target department stores between Thanksgiving and Black Friday's holiday shopping season in 2013. Allegedly, a teenage hacker using the code name Ree4 modified “run-of-the-mill” malware, renaming it “BlackPOS,” and sold the malicious code to eastern European cybercriminals. Instead of attacking Target directly, hackers sent malware-laced emails in a “spear phishing” attack to a third-party vendor with

access to Target's network. Once the hackers had access to vendor credentials, entry to Target appeared to come from a trusted source.

Once the hacker gained access to Target's network and its point of sales (POS) systems the malware waited to launch its attack. Between November 15 and 28, the hackers gained access to a small number of cash registers in Target stores and used this time to test their POS malware. By the end of November, the hackers had captured control of virtually all of Target's POS devices, collecting customer card data and transaction activity through December 2013.

The BlackPOS virus was identified as one of several POS malware attacks during the same holiday season. The method and scale of the attack on Target stood out owing to its design, making its data manipulations extremely hard to detect. The BlackPOS malware also exhibited other distinguishing behavior not seen before in that it made copies of the stolen data and stored the records on Target's own servers. To mask the attack further, the malware did not operate around the clock but limited its activity to the store's prime times between 10:00 am and 5:00 pm. The *New York Times* reported that the company was vulnerable to the cyberattack because its systems were "astonishingly open—lacking the virtual walls and motion detectors found in secure networks like many banks."^{*}

Was the sophistication and unique nature of the BlackPOS malware an appropriate test for situational awareness? How would situational awareness been helpful in detecting this devastating attack? Target maintained an extensive cybersecurity team that reportedly was well versed in addressing targeted attacks frequented on retailers. According to a Bloomberg article in March 2014, Target had installed monitoring devices from FireEye, a top cybersecurity firm, six months prior to the attack. Target's security team in Bangalore, India was alerted of a November 30 theft of customer data and the Bangalore security team notified security specialists in the United States, but then nothing happened.[†]

^{*} http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html?_r=2

[†] <http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>

Under testimony before Congress, Target testified that it was unaware of the theft until notified by the U.S. Department of Justice, prompting an investigation that led to the discovery of the alerts that had gone unaddressed in its computer logs. What is clear is that the opportunity for exercising situational awareness was missed if the security analyst's alerts were overlooked or delayed for inexplicable reasons. Cybersecurity professionals are constantly under the gun and must prioritize their time and resources for high target threats. After the fact, the omission was a damning indictment of poor situational awareness.

Pointing out missed opportunities is easy after the fact but a broad brush does not fully explain the challenges and issues faced by Target's security team. Hackers have become increasingly astute at exploiting cognitive blind spots by using very simple tricks to cover their tracks. Take into account the novelty of the BlackPOS malware and the entry point through a third-party provider; the cloaking behaviors used by the virus made it a challenge for early detection.

The lesson here is that an organization with formal security processes will find additional benefits by augmenting situational awareness and response in support of the security team. The security team in India performed its job but may have represented one of a larger number of alerts the home office needed to respond to during the course of the hack. Situational awareness protocols are used to validate threat assessments either systematically or manually to conclude the veracity of the risk. Cybercriminals understand how to exploit basic human behaviors and regularly test their assumptions through a variety of techniques. More advanced techniques increasingly involve the influence of a user's behavior and perception through the introduction of misinformation. This explains one reason why the attacks are harder to discover and, harder still, to assess the extent of the attack's damage, leading to delays in comprehensive remediation, if achieved at all. A Reuter's article reported that Target did not disclose the security breach until after a security blogger posted reports on his website and journalists called Target to verify the reports. Meanwhile, Neiman Marcus and several other undisclosed retailers experienced similar attack behavior during the same period, allowing hackers to take advantage of the delay in disclosure.

Suggestions for a "Cyberattack Data Clearinghouse" have not yet gained support. "Threat intelligence sharing is ineffective," concluded

a Department of Homeland Security survey reviewed by *Nextgov*.^{*} Nonetheless, the speed, scale, and asymmetry of attacks in use argue for a legally protected, early report/response mechanism to share attack behavior with industry verticals as early warning systems. These self-regulated groups, organized by industry vertical and cross-vertical channels, should include law enforcement and security advisers in ways that leverage leading practice and resources more efficiently.

The Securities and Exchange Commission (SEC) published CF Disclosure Guidance: Topic No. 2, on Cybersecurity in October 2011, which outlines its expectations for SEC registrants on public disclosure of a cyberattack, yet more is needed to help coordinate and facilitate the process of disclosure. Cyberattacks are typically executed with “bespoke,” or custom-designed, malware that is used once and discarded after disclosure. By the time other firms in the same industry learn of the attack and implement defenses to prevent similar attacks it is already too late. Situational awareness must be broader than isolated incidents within a firm if the information and data needed to evaluate threats are to be acquired in a timely manner.

Reluctance to report is considered common. Two retailers are reported to have “waited more than two years to admit that they were victims in 2007 of notorious hacker Albert Gonzalez, who was accused of masterminding the theft and reselling of millions of credit cards and ATM numbers,” according to the same Reuters report in January 2014. The reluctance to make public disclosure is understandable given the market reaction and subsequent fallout that ensues.

Target’s profit for the holiday shopping period fell 46% from the same quarter the year before; the number of transactions suffered its biggest decline since the retailer began reporting the statistic in 2008. Target also suffered a decline in sales of between 2% and 6% after disclosure and was the subject of lawsuits and legal costs negotiated with credit card holders and insurance carriers as a result of the cyber-attack. A *New York Times* article quotes one source as saying that the

^{*} “A Review of the Department of Homeland Security’s Missions and Performance,” A Report by Senator Tom Coburn Ranking Member Committee on Homeland Security and Governmental Affairs, U.S. Senate, 113th Congress, January 2015.

“total damage to banks and retailers” resulting from the Target network security breach “could exceed \$18 billion.”

The externalities of cyber risk are a difficult challenge to resolve but can and should be debated as part of the framework for addressing the long-term costs of cybercrime. The backstory of Target’s hack demonstrates how a firm’s lack of situational awareness creates self-inflicted damage. It should be noted that several firms suffered from a similar attack but Target’s negative press is, in part, a result of the size of the firm and damage caused by the hackers.

Situational awareness is an important component of the cognitive tool kit for cybersecurity professionals. The effectiveness of situational awareness is only as strong as the quality, completeness, and timeliness of the information and data observed in the environment. The weaknesses of situational awareness have been noted by researchers. “The test of Situation Awareness as a construct will be in its ability to be operationalized in terms of objective, clearly specified independent (stimulus manipulation) and dependent (response difference) variables . . . Otherwise, SA will be yet another buzzword to cloak scientists’ ignorance” (Flach, 1995, p. 155). Recognizing the inherent limitations, the lesson from Target should be that situational awareness cannot be taken lightly and must assume a role as part of an integrated program in organizations as an arsenal of tools to limit, deter, and/or prevent damage from an attack.

Researchers have only scratched the surface of the cognitive skills needed to enable asymmetric countermeasures in cybersecurity. One of the risks cited in situational awareness is complacency, “Assuming everything is under control affects vigilance. When things are slow, tasks are routine, and/or when objectives have been achieved, complacency can occur.”* This is prudent advice for all risk professionals and especially so for cybersecurity. It is now time to delve into a new field of research called Cognitive Security, Intelligence and Security Informatics (ISI) to see how it can be used to help enhance security measures. ISI involves a set of countermeasures to address cognitive hacking.

“Cognitive informatics is the multidisciplinary study of cognition and information sciences, which investigates human information

* <https://www.uscg.mil/auxiliary/training/tct/chap5.pdf>

processing mechanisms and processes and their engineering applications in computing,” according to Pacific Northwest National Laboratory (PNNL). PNNL’s research focuses on developing technologies to broaden the integration of human interface with technology to improve learning and decision making, among other benefits. Cognitive informatics is multidisciplinary in approach and is informed by research in psychology, behavioral science, neuroscience, artificial intelligence, and linguistics.

Security professionals are increasingly fighting new battles in cyberattacks against asymmetric weapons. The ease with which hackers continue to penetrate traditional defensive posture calls for a more robust set of measures using smart systems and a better understanding of the vulnerabilities at the intersection of the human–system integration. Training and awareness campaigns are still important but are woefully deficient. Even astute technology professionals are frequently fooled. A recent news account reported that Facebook founder Mark Zuckerberg’s social media accounts were hacked.* Zuckerberg’s accounts were compromised by a group called OurMine that took credit, claiming Zuckerberg’s credentials were discovered in a database of compromised LinkedIn accounts. This story highlights a simple truth about cyber risk that we take for granted. If we choose to actively engage social media, email, and other communications channels, each of us is responsible for our own security. However, when you choose to do so from your workplace you expose the firm to cyberattacks, unwittingly compromising investments in security for the entire firm. The hack of Zuckerberg’s social media accounts was an opportunistic and simple one executed to gain exposure for OurMine but should serve as a warning that we too leave a digital trail of data behind.

“Physical and syntactic attacks occur totally within the computing and networking infrastructure, seeking vulnerabilities, without the intervention of human interaction. A cognitive hack requires the *user* to change behavior via the introduction of misinformation that violates the integrity of the overall system.”† Cognitive hacks can take many

* <http://www.usatoday.com/story/tech/news/2016/06/06/mark-zuckerbergs-social-media-accounts-hacked/85477432/>

† <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.6587&rep=rep1&type=pdf>

forms, some of which do not involve an attack on network infrastructure, but may simply include “the provisioning of misinformation, the intentional distribution or insertion of false or misleading information intended to influence a reader’s decisions or activities,” according to Dr. Paul Thompson of the Thayer School of Engineering and Department of Computer Science at Dartmouth College.

Cognitive hacking continues to spread in ways that have yet to be fully defined. One definition describes it as follows. Cognitive hackers manipulate a user’s perception and rely on his or her changed actions to carry out the attack. Effective countermeasures must aim at preventing misinformation through authentication, collaborative filtering, and linguistic analysis. In 1981, Carl Landwehr observed that “Without a precise definition of what security means and how a computer can behave, it is meaningless to ask whether a particular computer system is secure.”* Landwehr’s point is that we must define security more precisely to account for the risks we wish to mitigate. The open nature of the Internet makes it an ideal medium for spreading misinformation. ISI is one example of how computer scientists are pushing the boundaries of security to advance countermeasures in cognitive and semantic attacks to build trust back into networked information systems.†

The concept of cognitive hacking, ISI, as the name implies, is a cross fertilization of several disciplines currently gaining traction. Security informatics serves as the core platform for delivery of countermeasures to semantic attacks. Why focus on semantic attacks? Semantic attacks are characterized as campaigns that use misinformation and deception to successfully evade the defenses of organizations. The goal of the attacker is to hack the mind of the user cognitively to influence the user’s perception and behavior. Think of a cognitive hack as one of the methods a hacker uses as a countermeasure to obscure situational awareness. The obvious result is gaining permission to enter the organization around its own defenses.

Cognitive hacks are simple, easy to deploy, and most importantly, effective. For example, if you have ever gotten an unsolicited email asking you to click on a link to address a problem with an old bankcard

* <http://www.ists.dartmouth.edu/docs/ch.doc>

† <http://dl.acm.org/citation.cfm?id=2500948>

account you no longer use you may have unknowingly been the victim of a cognitive hack. Social media has also become a popular source for hackers who pose as HR recruiters, using links to factious job postings luring the user to set up personal profile accounts only to be used by hackers to exploit personal information for future attacks.

Schneier describes a semantic attack as “attacks that target how, we as humans, assign value to content.” Schneier considered “the human/computer interface as the least secure interface on the internet.”* Semantic countermeasures (behavioral algorithms) are also considered ideally suited to address insider threats, an important focus in security. Semantic attack vectors are more subtle and covert, differing from brute force attacks that require security professionals to defend against attacks using intelligence methods to measure trusted sources.

In July 2010, in a real-life example, the Associated Press (AP) uncovered a semantic hack through a U.S. government-funded effort to create a Twitter-like social network in Cuba called ZunZuneo. It was quite a success, shutting down only after it became too big, too fast. The humanitarian agency behind the project—United States Agency for International Development (USAID)—said, “It just wanted to create a network where users could talk among themselves.” The Associated Press article was picked up broadly, including in the *Washington Post*, and caused a row in political circles upon its disclosure. The optics of the details disclosed by the AP article prompted a public response by USAID, the governmental development agency that created the website.

USAID posted a statement on its website, dated Thursday, April 2, 2014. In reference to the AP article on “Cuban Twitter” on April 3, 2014, USAID spokesperson Matt Herrick issued the following statement:

It is longstanding U.S. policy to help Cubans increase the ability to communicate with each other and with the outside world. Working with resources provided by Congress for exactly this purpose. USAID is proud of its work in Cuba to provide basic humanitarian assistance, promote human rights and universal freedoms, and to help information flow more freely to the Cuban people. All of our work in Cuba,

* <http://www.counterpane.com/crypto-gram-0010.html>

including this project, was reviewed in detail in 2013 by the Government Accountability Office and found to be consistent with U.S. law and appropriate under oversight controls.

It is also no secret that in hostile environments, governments take steps to protect the partners we are working with on the ground. The purpose of the ZunZuneo was to create a platform for Cubans to speak freely among themselves, period. At the initial stages, the grantee sent tech news, sports scores, weather, and trivia to build interest and engage Cubans. After that, Cubans were able to talk among themselves, and we are proud of that. USAID is a development agency and we work all over the world to help people exercise their universal rights and freedoms.*

Cognitive hacks have been around for some time but the sophistication of the attack has grown. In August 2000, a press release became widely circulated in major media news sources reporting that Emulex, a server and storage provider, had revised earnings from a \$0.25 per share gain to a \$0.15 loss and lowered net earnings from the previous quarter. Emulex shares plummeted more than 50% within minutes of the release, from \$104 to \$43 per share. The story was totally fabricated by a 23-year-old hacker named Mark Jacob who had previously lost \$100,000 in a short sale trade. The hack was an attempt to recover his losses, which he did fourfold, until his indictment for securities fraud. Jacob was able to achieve his hack outside of the domain of a computer network through the use of manipulation and deception to change the perception of investors. “The internet’s open environment makes it ideal for hackers to launch a variety of semantic attacks.”†

Semantic attacks are defined as the execution of the delivery of misinformation through the use of various media, including the Internet, to create the impression of a trusted source for the sole purpose of changing behavior. The real difference in semantic attacks, as opposed to other forms of cyberattacks, is that the user is the target of the attack, in contrast to the network (physical attack) or operating logic (syntactic attack) of the hardware. The Cuban ZunZuneo and the Mark Jacob stock scheme are examples of semantic attacks.

* https://www.washingtonpost.com/lifestyle/style/usaaid-effort-to-undermine-cuban-government-with-fake-twitter-another-anti-castro-failure/2014/04/03/c0142cc0-bb75-11e3-9a05-c739f29ccb08_story.html

† <http://www.ists.dartmouth.edu/library/300.pdf>

Many people recognize “phishing” as one of the most common types of semantic attacks but it’s clearly not the only one. A newer version of semantic attacks has begun to emerge called “malvertisement.” A malvertisement is an online advertisement that is infected with a virus or malicious computer code, which takes advantage of placement of online advertising to steadily disperse malware to new users. Semantic attacks have proven very effective in the past; however, as Internet users have become more aware of these tricks hackers continue to evolve.

Cyberattacks aimed at organizations have increased since 2009, with 91% of all organizations hit by cyberattacks in 2013.* The vast majority of organizations rely heavily on email for internal and external communication. Thus, email has become a very attractive platform from which to initiate cyberattacks against organizations. Attackers often use social engineering to encourage recipients to press a link or open a malicious webpage or attachment. According to Trend Micro, attacks, particularly those against government agencies and large corporations, are largely dependent on spear-phishing emails.

Social media, popular video websites, and church and dating websites have increasingly become platforms used by cybercriminals to execute malware. The goal remains the same for hackers but the tactics are less transparent to web surfers. It is easy to see that the diversity of cognitive and semantic hacks requires an entirely new set of tools and why a defensive strategy is ineffective in preventing, correcting, or detecting cognitive hacks. The good news is that promising early stage defensive and offensive strategies are being developed to deal with cognitive hacking.

In response to the rise of semantic hacks, a community has emerged from a very diverse set of disciplines to explore scientific approaches to cybersecurity. Collectively, a new science is evolving called Cognitive Security (CogSec). Consider cognitive security a tree with many branches, each focused on solving security at the human-machine intersection. There is growing recognition that cybersecurity requires advanced approaches, similar to the ones used by hackers, to counter the sophistication of this elusive adversary. One of the largest and most active branches of CogSec is found in the research on ISI.

* <http://www.humanipo.com/news/37983/91-of-organisations-hit-by-cyber>

New research in ISI is advancing rapidly into a cross-disciplinary field of study focused on human interactions in cyberspace. ISI is an interdisciplinary approach that includes research topics in information technologies, computer science, public policy, bioinformatics, and social and behavior science, and involves academic researchers as well as local, state, and federal law enforcement and intelligence experts and other intelligence agencies in support of counterterrorism and homeland security missions geared toward prevention, preparedness, and response to terrorist acts.

Since 2005, the ISI research community has been advancing an impressive array of research results that are both technically innovative and practically relevant. ISI uses computational approaches to automate the extraction of causal knowledge and social behavior of, say, a terrorist organization from online textual data. The types of causal knowledge and social behavior include actions, preconditions and effects, and action hierarchy. Examples include the monitoring and evaluation of social media and other online conversations between terrorist and other bad actors to understand changes in group behavior to assess threats associated with terrorist groups and within the hacker community.

ISI is closely associated with law enforcement and military cyber defensive strategies, but that is beginning to change. Similar methods are developing in parallel in the private sector and increasingly being used in vendor platforms as advanced security counter-defense measures. Private security vendors are also developing new tools to address threats, such as insider threat and deception detection software using behavioral algorithms. Demand for more effective security will continue to grow as more advanced and persistent threats rise sharply. Manual processes are less effective against a high volume of asymmetric attacks used today. Researchers are also exploring a variety of security methods in recognition of the challenge of developing effective machine learning systems.

Let's stop for a moment to understand better the topic of machine learning. The term "machine learning" is often tossed around very loosely in the marketing of vendor cybersecurity services with as much hype and mystery as "big data." So let's be very clear about the current state of machine learning and its limits today to gauge the benefits of further research to come. Machine learning is real and is

being used successfully in certain applications such as Google's driverless cars, to predict fraud, detect terrorist activity, and recommend products to customers. Machine learning requires technology applied to huge quantities of data and interdisciplinary expertise in statistics, data mining, machine learning, artificial intelligence, cybersecurity, and more.

There are four types of machine learning algorithms organized around a taxonomy used to produce a desired outcome for each type: (1) supervised learning; (2) unsupervised learning; (3) semisupervised learning; and (4) reinforcement learning. "Supervised learning is the most common type used by 70 percent of algorithms," according to Wayne Thompson, manager of data science technologies at SAS. Supervised learning is "trained" using examples where the desired outcome is known. Unsupervised learning is used in approximately 10% to 20% of machine learning algorithms. The algorithms are not "trained" to find the right answer but instead must find the hidden patterns or structure in data. Semisupervised learning is a hybrid approach using both supervised learning and unsupervised learning techniques to "train" algorithms using a ratio of each approach. Finally, with reinforcement learning the algorithm discovers for itself which actions yield the greatest rewards through trial and error. Reinforcement algorithms require three components: the agent—the learner or decision maker; the environment—everything the agent interacts with; and actions—what the agent can do with the data.

Regardless of the methods used, the algorithm requires an iterative cycle of trial and error to develop predictive models over time. Adjustments are made by data scientists to find the right fit of parameters to gain confidence in the model's predictive capabilities. A small number of large firms are using big data for cybersecurity. According to a 2014 Microsoft survey of security executives, only 16% of sample firms have active programs in place and are in early stage development. Respondents in the survey plan to focus on user activity (insider threat), external threats, network traffic, policy violations, endpoints, and application behavior. Microsoft's survey does not address how the respondents determined their priority ranking of areas of focus nor explain whether their assumptions changed after conducting an analysis of data. The Ponemon Institute facilitated the survey.

One clear implied outcome from the Microsoft survey and SAS's modeling exercise in cyber analytics is the need for analytical skills in IT security to build these programs in-house. The math is complicated and is still developing as researchers learn how to transfer success from other disciplines to cybersecurity. Firms that use vendors to design and build their programs will be dependent on consultants until a new discipline is created in-house. The costs and time needed to build these skills are available to the largest firms but how will smaller, less financially capable firms fare in the race to cognitive security? There is more good news on that front as well. Cyber education is growing and funded in partnership with grants by government, private, and public capital and institutions of higher education. In time, a new cadre of cybersecurity experts will contribute to new advances in security.

"The IEEE International Conference (ISI) on Intelligence and Security Informatics has evolved from its traditional orientation of intelligence and security domain towards a more integrated alignment of multiple domains, including technology, human cognition, organizations, and security. The scientific community has increasingly recognized the need to address intelligence and security threats by understanding the interrelationships between these different components, and by integrating recent advances from different domains," according to the IEEE website.*

Four main verticals have emerged as key disciplines in ISI: Data Science and Analytics in Security Informatics; Security Infrastructure and Tools; Human Behavior in the Security Applications; and Organizational, National, and International Issues in Counter-terrorism or Security Protection. IEEE has prioritized research submissions across each of these disciplines to focus resources and thought leadership.

IEEE is the self-described "world's largest technical professional organization dedicated to advancing technology for the benefit of humanity."[†] The organization promotes research publications and standards in cybersecurity, conducts conferences and educational events, and has a global membership and focus. However, as you can

* <http://isi2015.wixsite.com/isi-2015>

† <https://duckduckgo.com/?q=cybersecurity+associations&t=ffab>

imagine, a growing number of cybersecurity course providers have exploded onto the scene with constituent groups ranging from educators, Homeland Security, space, military, industry, telecommunications, trade associations, and many more.

Cybersecurity talent is in high demand, with higher education, nonprofit and for-profit organizations experiencing a surge in new entrants into the field. As the number of professional and corporate trained cyber hackers and security professionals grow in the coming decades, the need for a more advanced cyber governance and risk management framework is needed to account for cyber ethics and cyber law in a world with people who possess the skills to hack into any system.*

The Association for the Advancement of Artificial Intelligence, in cooperation with Stanford University, has sponsored a series of symposiums in computer research bringing alive the vision of exploring the interaction between humans and machines. The most recent series put forth seven symposia on Artificial Intelligence (AI) and the Mitigation of Human Error, Multiagent Learning, Social Intelligent Human–Robot Interactions, Intelligent Systems for Team Work, Ethical & Moral Considerations in Non-Human Agents, Studies in Social Media and Human-Generated Content, and Well-Being Computing. Previous series have been equally diverse, with topics such as “Social Hacking and Cognitive Security on the Internet and New Media” and “the Intersection of Robust Intelligence and Trust in Autonomous Systems.” Large tech firms have already begun branding their cognitive security offerings along with private equity joining the fray with rounds of acquisitions in anticipation of high adoption rates in the near future. Cognitive security is being touted beyond cybersecurity, with some vendors making the case for its use in managing energy; however, I suspect this will expand rapidly to enterprise risk, integrating compliance, risk, audit, IT security, and more.

Security professionals need to develop new processes in preparation for the emerging cognitive security environment being developed. The building blocks that lead to a cognitive risk program include considerations on three dimensions: *data management and analysis*, *technology redesign*, and *cognitive risk at the human–machine interaction*. The final

* <https://duckduckgo.com/?q=university+associated+cyber+security+initiatives&t=ffab>

chapter will go into some detail for developing a “bridge” from today’s defensive strategy of hardening the enterprise to an active cognitive risk framework. The first step in the transition to a new environment starts with a conversation about risk. Although this may sound intuitive, conversations about risk and uncertainty are more complex than most believe.

The topic of risk is made more complex by counterintuitive factors we each take for granted. The first of these factors is language. Earlier I mentioned the conversation between Apple and the director of the FBI. Each side framed the risk, access to meta-intelligence, differently without reconciling outcomes to expectations on both sides. Conflicting views of risk are a natural result of unresolved differences in how each side views a risk, leading to distrust. The language of risk is a major reason organizations develop “blind spots” to certain risks, resulting in a failure to move their risk program forward. These blind spots are avoidable but predictable, as displayed in the public debate about the iPhone®.

Heuristics are the shortcuts we use to solve complex problems when simple answers are not available. Heuristics and intuition may lead to errors in judgment because the processes are often unconscious, leading to a failure to see the mistakes we make in our analysis. Behavioral and cognitive science makes us more aware of these unconscious failings, allowing security and risk professionals to recognize the pitfalls and make corrective adjustments before communications deteriorate.

By understanding the role of human behavior and leveraging behavioral science findings, the designers, developers, and engineers of information infrastructure can address real and perceived obstacles to productivity and provide more effective security (Predd et al., 2008; Pfleeger et al., 2010). There is growing evidence to suggest the importance of including some element of human behavior into security systems, but what does that mean exactly? Initial studies have focused on several areas of interest, including how trust is established on the web, changes in employee compliance (Lerner and Tiedens, 2006), the effect of emotional stressors (Klein and Salas, 2001), and other effects outside of the norms of behavior.

A balance has yet to be struck between traditional security measures and behavioral concepts. The aforementioned studies point to a focus on internal behavior, specifically targeted at the insider

threat. Several authors have suggested that the insider represents the largest threat actor; however, this metric should be taken with a grain of salt. The focus on internal threats that are now easier to recall because of Edward Snowden leaves firms exposed to even greater risk. Availability bias is the belief that easy to find data or the frequency of recent data validates the proof of a belief. Edward Snowden has become the main threat in cybersecurity without quantifiable data to prove this is a universal risk. Snowden is a tail risk: huge impact, low probability risk. Let's call this the "Edward Snowden" effect, after the former CIA employee and National Security Agency contractor who disclosed the government's global surveillance program. This is not to say that insiders do not represent a threat; the question is whether it should be considered the highest risk. Insiders' access to customer and business data represents a risk that is more easily identifiable and preventable with routine internal controls and surveillance. The cyber threat, on the other hand, is by definition a higher risk given the lack of foreknowledge of the vulnerability or the means by which the attacker is able to steal data.

The risk of confirmation bias from high-profile events may lead to a narrowing of focus on known threats at the expense of missing the circumstances leading up to new vulnerabilities in the future. Libicki and Pfleeger (2004) have documented the difficulties in "collecting the dots" before an analyst can take the next step to connect them. If a "dot" is not as visible as it should be, it can be overlooked or given insufficient attention during subsequent analysis.

One such "dot" is the entry of millennials into the workforce. As the workforce of the future changes from baby boomers to millennials, the risk of semantic attacks is becoming more acute. Millennials are more adept at engaging in a variety of social media sites from work and through mobile devices, exposing themselves and their employers to cyber hacking. With the proliferation of social "news" outlets for content and the perceived safety of sharing personal data online by millennials, social media has become an easy target in cyberattacks. As mentioned previously, Mark Zuckerberg, an uber millennial who is tech savvy, had his social media account hacked using an old password from LinkedIn, another social media platform. Millennials are more likely to trust these online services, having known few other

alternatives, making this generation more susceptible to cyber risks in the future.

Millennials have adopted entirely different trust models than their baby boom predecessors who spent less time searching the web for their news and entertainment. The millennial generation, broadly defined as this generation's early teens to mid-30s adults, represent roughly 25% of the U.S. population and are the first generation of Americans born in the mobile digital age. Websites such as Facebook and Google are perceived by millennials as the utility of their day. Mobile apps, media, and other digital content is taken for granted given 1 billion+ people globally use these platforms. Millennials take security for granted as well, but should they?

As technology converts old industry to new eCommerce platforms ranging from how we pay for products and services to ordering custom-made clothing and more, we expose ourselves without the assurance of trust on the Internet. Interestingly, organizations have evidence of the threats of social media yet are reluctant to prevent access and instead have expanded vulnerability with the issuance of mobile phones and other communication devices, leaving firms more exposed. These too are the contradictions in cybersecurity. Simple measures can be taken without huge expense but the "blind spots" persist.

Trust must be redefined as technology accelerates at an unprecedented speed. Big tech firms, in collaboration with industry leaders, are developing entirely new customer interface platforms using robots with AI, machine learning, and voice response systems that learn from interactions on the web, changing our perception of trust. Mark Zuckerberg's Facebook is one of the first big tech firms to deploy chatbots for business users on a large scale. "Facebook boasts more than one billion messages are sent between businesses and users via Messenger," according to an April 2016 *Fortune* article.* Several technology developers are experimenting with chatbot personalities, including Microsoft's now infamous "Tay," who learned how to become a racist from Twitter users. Microsoft's experience with Tay should teach us very valuable lessons about the need for safeguards when using AI in the public domain and points to the inherent limitations that still exist.

* <http://fortune.com/2016/04/12/facebook-chat-bots-messenger-app/>

A user's ability to discern trust accurately is complicated by the diversity of user-generated content and a plethora of disruptive entrants in the marketplace of ideas for media and digital content. As traditional news outlets of trusted content increasingly transition to today's 24/7 digital content, the line of trust on the web will blur further. In my opinion, today's social media dominated content is much less trustworthy, exposing users and organizations to higher risk and may help to explain, in part, the accelerated growth of cyberattacks. As user adoption of new technology grows, we are exposed to more opportunities for an attack without our knowledge.

According to a 2014 Symantec Internet Security Threat Report, "the primary motive behind social networking attacks is monetary gain." The report outlines that phishing attacks are evolving, "moving further away from email and into the social media landscape." Nonetheless, the same techniques that security professionals have observed in phishing and spam emails are being leveraged in social media campaigns.* Cognitive hacks are disguised as "fake offers," "fake Like buttons or Likejacking," "fake plugins or Internet extensions," and "fake apps." Given this trend, the definition of security must be reexamined to combat diminished trust at the human-machine interaction. Stakeholders, from content and solution providers to security analysts, must evaluate how to restore trust on the Internet. A concerted effort is needed by all parties to narrow the corridor of risk against a persistent and growing community of sophisticated adversaries.

How does a corporate security analyst assess the trustworthiness of content among a universe of social media sites via a mobile "bring your own device" (BYOD) environment? Social media is a global phenomenon that blurs the lines of trust in personal and business relationships. In a December 2014 report by Cylance, an endpoint security firm investigated an Iranian base of attackers operating undetected for at least two years before discovery. "The attackers, dubbed "Threat Group-2889" or "TG-2889," appeared to be Iranian-sponsored hackers whose activities were documented by the security company in a December 2014 report investigating a campaign called "Operation

* <http://www.securityweek.com/next-big-cybercrime-vector-social-media>

Cleaver.”* The attackers set up at least 25 fake LinkedIn accounts, creating personas, photographs, and information from well-known corporations in the United States, South Korea, and Kuwait, among other countries.

“Perhaps the most chilling evidence collected in this campaign was the targeting and compromise of transportation networks and systems such as airlines and airports in South Korea, Saudi Arabia and Pakistan,” according to the Cylance report. “The level of access seemed ubiquitous: Active Directory domains were fully compromised, along with entire Cisco Edge switches, routers, and internal networking infrastructure. Fully compromised VPN credentials meant their entire remote access infrastructure and supply chain was under the control of the Cleaver team, allowing permanent persistence under compromised credentials. They achieved complete access to airport gates and their security control systems, potentially allowing them to spoof gate credentials. They gained access to PayPal and Go Daddy credentials, allowing them to make fraudulent purchases and allowed unfettered access to the victim’s domains.”

The group behind Operation Cleaver had been active (on LinkedIn) since at least 2012, targeting more than 50 companies across 16 countries, including organizations in the military, government, oil and gas, energy and utilities, chemical, transportation, healthcare, education, telecommunications, technology, aerospace, and defense sectors. The remaining fake accounts were set up as supporting personas to give the key players credibility and believability within the site. The hackers posed as executive recruiters to approach members on the site and may have used spear phishing and malicious web links to increase their success rate.

This attack was not the first of its kind. “In May 2014, cyber intelligence company iSIGHT Partners analyzed a campaign in which attackers had used over a dozen fake personas on various social networking websites.”† It is shocking to believe that such a massive attack was achieved so simply using syntactic and semantic methods.

* <http://www.securityweek.com/iranian-sponsored-hackers-hit-critical-infrastructure-companies-research>

† <http://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation>

“Simplicity of approach” and “simplicity of execution” are recurring themes in each of the major attacks we have reviewed. Simplicity is used to gain trust, obscuring the intent of hackers and allowing them to trick users into changing their behavior.

Researchers have also formulated general themes about the interaction of cybersecurity and cognitive risks. The first theme, as we have discussed, is improving human–machine interactions using technology to determine the trustworthiness of the interaction. Second, security analysts, overloaded by the sheer volume of threats large and small, suffer from *cognitive load*, leading to a diminished ability to process all of the threats efficiently with the appropriate level of prioritization. Researchers are exploring new approaches to augment the highest priority threats needing the attention of security professionals (Miller, 1956; Chase and Simon, 1973; Mack and Rock, 1998; Burke, 2010).

Simons and Chabris (1999) and Simons and Jensen (2009) later identified the effects of cognitive load more succinctly as *inattentional blindness*, referring to a person’s inability to notice unexpected events when concentrating on a primary task. Third, researchers noted significant cognitive bias in security professionals resulting in vast differences in how one analyst perceives a threat versus others. Each threat can be experienced differently when factors such as aptitude, training, or inability are taken into account. These factors are called heuristics, a main cause of misconception in the judgment of risk. Humans develop expertise and gain experience by knowing what to do when faced with similar experiences. When the experience is out of the ordinary these same skills tend to fail us simply because we have not prepared nor have the skills to adjust. This is not a personal failure; it is a natural result of ineptness. This is why we need to improve the language of risk. Ineptness is most often used in a negative connotation when someone fails to recognize what others see as obvious, often after the fact. Ineptness is a signal that either additional training is needed or a different set of tools is required to address uncommon risks. And, lastly, lacking a quantitative approach to threat assessment, security analysts are unable to measure risks uniformly, settling on qualitative measures of likelihood and impact that are inherently inaccurate, producing wide variance in over- and underestimations of risks.

Hold on! If technology is not enough and humans can't be trusted, how do we build intuitive situational awareness in cyber defense? The Apple ecosystem is a good proxy for system engineering design. Simplicity, intuitive integration and functionality allowed Steve Jobs to reinvent the mobile phone into a smartphone. Cybersecurity requires additional elements but the concepts are applicable. Layered security technology must be redesigned into smart cybersecurity.

The genius of Steve Jobs is in how he transformed function into simple utility. The smartphone's form changed incrementally but its utility is remarkable. Jobs was fanatical about details; he instinctively understood how cognition operates on two levels: intuition (heuristics and biases) and analytical concepts that require more time and energy. The more time, energy, and mental resources needed to solve a problem the less likely the outcomes are uniform. Jobs reimaged the smartphone to make it simple and intuitive. A small child can pick up an iPhone and begin to use it. BlackBerry, on the other hand, struggles to compete with the iPhone's simplicity. If we want humans to do a better job at cybersecurity we have only two options. First, make security simple and intuitive for the human mind or use computer technology to correct and avoid errors in human judgment. Let's address the second problem first and return to the first problem near the end of this chapter.

Having already introduced cognitive security, let's return to this topic to look more deeply into the areas associated with human limitations in managing cognitive hacks. Computer scientists and researchers are producing impressive results in the field of AI as a proxy for how technology will be used to simplify security by integrating machine learning and cyber defense capability.

AI solves a number of disparate problems and creates new challenges as well. According to Google researchers, the process for creating machine learning and AI is labor intensive: "we gather large volumes of direct or indirect evidence of relationships of interest, and we apply learning algorithms to generalize from that evidence to new cases of interest. Machine Learning at Google raises deep scientific and engineering challenges. Contrary to much of current theory and practice, the statistics of the data we observe shifts very rapidly, the features of interest change as well, and the volume of data often precludes the use of standard single-machine training algorithms. When

learning systems are placed at the core of interactive services in a rapidly changing and sometimes adversarial environment, statistical models need to be combined with ideas from control and game theory, for example when using learning in auction algorithms.”*

What is AI and how does it work? AI falls into two or three camps depending on your definition. *Strong AI* (sometimes called General AI) aims to duplicate human intellect: to understand, perceive, have beliefs, and exhibit other cognitive traits normally ascribed to human beings. Strong AI has not been achieved and many believe it is not necessary as long as certain tasks can be performed to get work done. However, there is a great deal of research and controversy surrounding the topic of replicating human intelligence. Suffice it to say, Strong AI is not used for cybersecurity. The second form of AI is called *Weak AI*. IBM’s Deep Blue, known for beating chess masters, is a form of Weak AI, which is at most a simulation of a cognitive process but is not itself a cognitive process. The third version is a hybrid of the two called *Narrow AI*, a branch of Weak AI with subsets of sophistication from the very simple (Apple’s Siri®) to more complex learning algorithms. In fact, hackers are using Narrow AI in remotely controlled botnets to execute a variety of attack strategies very successfully. Google has demonstrated how “deep learning” systems function by learning layers of representations for tasks such as image and speech recognition. According to Google researchers, “reinforcement learning algorithms can learn to map which actions lead to the best outcomes, they are ‘model-free,’ meaning the system knows nothing about its world.”† Google’s DeepMind team designed AlphaGo, described as an intuitive system that beat the European Go Champion and elite player Fan Hui. AlphaGo was taught how to play Go by feeding its neural networks with 30 million Go games played by experts. Go, an abstract strategy board game invented in China 2,500 years ago, is considered to be the most complex board game, with 200 moves per turn versus 20 in chess and more iterations of play than the observable atoms in the universe.

* <http://research.google.com/pubs/ArtificialIntelligenceandMachineLearning.html>

† <https://www.technologyreview.com/s/601139/how-google-plans-to-solve-artificial-intelligence/>

Dr. Simon Stringer, director of the Oxford Centre for Theoretical Neuroscience and Artificial Intelligence, said that “AlphaGo and other deep learning systems are good at specific tasks—be that spotting objects or animals in photos or mastering a game. But these systems work very differently from the human brain and shouldn’t be viewed as representing progress towards developing a general, human-like intelligence—which he believes requires an approach guided by biology.”*

Deep learning is expected to hold the most promise for a wide range of business applications. In fact, there has been explosive growth in the number of software vendors touting their version of “AI or machine learning” capability, ranging from small entrepreneurs to the largest tech firms. The state of art in AI and machine learning will advance and each improvement must be understood by security professionals to determine the appropriate application of these tools in their cybersecurity practice. The science is advancing rapidly but is not mature enough to apply broadly without a considerable amount of legwork still needed to effectively combat cybercrime. One of the areas where intelligent, autonomous agents have shown a great deal of promise in cyberspace is in the area of deception detection.

Early versions of deception detection have focused on building trust relationships through a history of interactions. More recent research is concerned with applying models of cognitive and behavioral science to a group of intelligent agents, testing the correlation of deception and detection separately among the test group to determine whether intelligent agents can distinguish deception among its members.

Researchers have moved from the lab to real-world applications in deception detection AI capability. A team from MIT claims to have built an AI system that can detect 85% of cyberattacks with high accuracy.† “The new system does not just rely on the artificial intelligence (AI), but also on human input, which researchers call Analyst Intuition (AI), which is why it has been given the name of *Artificial Intelligence Squared* or *AI²*.” AI is used to scan more than 3.6 billion lines of log files and presents its findings to an analyst each day. The analyst reviews the data and then identifies which events are positive

* <http://www.techrepublic.com/article/how-googles-ai-breakthroughs-are-putting-us-on-a-path-to-narrow-ai/>

† <http://thehackernews.com/2016/04/artificial-intelligence-cyber-security.html>

for cyberattacks and discards the false-positive events that serve as learning for the AI system on each iteration. The researchers claim higher accuracy in cyber threat detection with each cycle of learning.

AI comprises a diverse subfield of research and practical applications, many so pervasive that observers no longer consider its use AI. To date, simple examples of learning have proven far easier to simulate using computers than the complex nature of human learning. Teaching machines to become expert in more than one area requires a quantum leap in speed, access to data, and algorithms for continuous learning. However, a great deal of progress has been made toward solving these problems. Wide use of intelligent decision support is still a distant goal, albeit the gap is closing rapidly.

Enn Tyugu, a researcher with Cooperative Cyber Defense Center of Excellence, wrote a brief review of potential AI application capability for use in cyber defense. Tyugu zeroed in on the need and challenges of operationalizing AI for cyber defense. “The applications are grouped in categories such as, neural networks, expert systems, search, machine learning, data mining and constraint solving.”*

Why is this important? The defensive posture of security professionals will only become more daunting as cybercriminals begin to implement their own form of AI algorithms more broadly.

“The main task facing artificial intelligence [AI] researchers at present is to create an autonomous, AI device fully capable of learning, making informed decisions and modifying its own behavioral patterns in response to external stimuli. It is possible to build highly specialized bespoke systems; it is also possible to build more universal and complex AI, however, such systems are always based upon the limited experience and knowledge of humans in the form of behavioral examples, rules or algorithms.”† Inevitably, domain-specific solutions will be linked together to create networks of knowledge that begin to operate in an autonomous fashion.

Why is it so difficult to create autonomous AI? “In order to perform work, AI currently requires algorithms that have been predetermined

* <https://ccdcoe.org/publications/2011proceedings/ArtificialIntelligenceInCyberDefense-Tyugu.pdf>

† <https://securelist.com/analysis/publications/36325/cyber-expert-artificial-intelligence-in-the-realms-of-it-security/>

by humans. Nevertheless, attempts to reach the holy grail of true AI are constantly being made and some of them are showing signs of success.”* The idea of autonomous weapons in cyberspace has a great deal of appeal; however, there are an equal number of distractors who worry that rapid development of technology in what is called the “Big Four” pose great risks as well. What are the Big Four? Pervasive Computing, Big Data Analytics, Artificial Intelligence, and Cyber Hostility define what one author called the “Four Horsemen of Datapocalypse.”†

Why such a dire view of the future in cyberspace? Pervasive computing is descriptive of a concept in which computing is embedded in our work, our play and entertainment, and social interactions. Think of social media sites and the wealth of personal and business data freely surrendered to everyone from around the world as an example. One can easily imagine a world where the integration of social media, entertainment, and business interactions will become indistinguishable. The Internet of Things (IoT) is but one promised version of this virtual world of connectedness. We are creating an artificial world that now rivals the real world in the infrastructure we rely on, services we purchase, and relationships we nurture in virtual networks. Pandora’s box has been opened and we can no longer go back and reverse course. Our personal data are now exposed in ways most people have little knowledge of or understanding.

The fear is that attacks can be initiated from anywhere in the world by unknown assailants with increasingly more sophisticated tools. The hack on the CIA chief’s email account in October 2015 demonstrates that governments are not in a position to protect us from threats on the web. Internet users are responsible for their own safety when surfing the web and that requires more than education and an understanding of new technologies. Going forward, humans need intelligent agents working behind the scenes helping to defend us in cyberspace because we cannot do so alone. The challenges are not insurmountable and will be overcome in time. What may be more challenging is the development of a framework for humans to engage

* <https://securelist.com/analysis/publications/36325/cyber-expert-artificial-intelligence-in-the-realms-of-it-security/>

† <http://artificialtimes.com/blog/why-should-we-care-part-1/>

in the management of autonomous systems through good governance and legal considerations. The imagination does not have to wonder far to envision how government officials, business leaders, and others could manipulate these tools.

What are the exposures? Social media presents a treasure trove of data about what we like, what we buy, how we spend our time, and a host of other information that can be used for surveillance of citizens with the use of big data analytics. However, the deep web, represented by data stored behind firewalls, in networks and storage devices used by government, medical, business, and personal users increasingly is exposed to attack. Internet users currently, wittingly or unwittingly, accept these risks given the small percentage of victims actually experiencing known breaches of security. As these numbers continue to grow, expectations for more elaborate security will be demanded. Trends in ransomware serve as one example of disturbing new trends in cyber theft used by hackers.

Ransomware is the latest example of sophisticated malware used by cybercriminals. It targets police departments, banks, hospitals, and mobile phones, encrypting parts of a computer, device, or an entire business network until users pay using Bitcoin in the hope, but not guarantee, of freeing their data from the criminal. In some cases a small ransom is paid, as was the case with a police department in Tewksbury, Massachusetts; others have paid higher amounts. Disturbingly, security professionals and the FBI have recommended negotiating with criminals and setting up a budget for the practice. More proactive methods are needed to defend against this growing threat. Seventy-four percent of security professionals in a 2014 ThreatTrack survey of 250 analysts responded they had been the target of cyber extortion and many have given up and paid a ransom to free their data. Ransom amounts have been small enough that the inconvenience and cost of system remediation have proven to be a successful business endeavor for entrepreneurial hackers. Flashpoint, an intelligence research firm, followed one Russian hacker's ransomware campaign and estimated his or her annual income was \$90,000 per year. The hacker employed a small team of surrogates who presumably deployed botnets in a ring of ransomware theft.*

* <https://www.helpnetsecurity.com/2016/06/02/ransomware-boss-earns-90000/>

Ransomware attacks are growing. Security researchers from Kaspersky Labs reported a Trojan program, Svpeng, used on Russia's three largest banks was initiated from Google Play to collect users' data. "When instructed by its server, the malware attempted to block the user's phone and displayed a message demanding payment of a US\$500 'fee' for alleged criminal activity."* That ransomware function was further improved and a new variant of Svpeng was identified on mobile phones outside of Russia. Ninety-one percent of users affected by the new version were based in the United States, but the malware also infected devices in the United Kingdom, Switzerland, Germany, India, and Russia, noted a Kaspersky risk analyst.

JP Morgan promised to double spending for risk management and security from \$250 million to \$500 million. Half a billion dollars is a tidy sum that will inevitably grow if better alternatives are not developed. The "cyber paradox" is exemplified as the endless cycle of massive spending on cybersecurity with no evidence of risk reduction in security. Going forward, the question of how to solve the cyber paradox remains. Will an integration of offensive and defensive security measures using some form of AI and machine learning make a difference? Clearly we can no longer continue to take incremental approaches in response to each cyberattack. But each time the stakes are raised hackers respond with even more sophisticated workarounds. Cyberwarfare has an analogy in conventional war, with each side seeking advantage through intelligence gathering on tactics and strategy. Defensive technologies, such as encryption, created to protect our data have become weapons used to hold business and individuals hostage. It is also clear that cyber skills are fungible; as new technology and techniques become known in the public domain hackers are as likely to adopt them as are security professionals. In response, security professionals need intelligence gathering to inform not only their response but also any adjustments required under certain threat conditions. Equally important is the need for security providers to consider how their products and services might be used or modified by those with the intent to harm others.

* <http://www.pcworld.com/article/2362980/russian-mobile-banking-trojan-gets-ransomware-features-starts-targeting-us-users.html>

The cyber paradox is also confounded by the lack of a sense of urgency by the general public to the threats of cybercrime. Warnings and training programs on the risk of cyber threats have proven ineffective, baffling law enforcement and security professionals alike. I have coined this phenomenon “risk deafness” to explain why this happens, supported by research. Education and awareness alone have many drawbacks and have proven to be ineffective tools in cyber risk and risk management more broadly. Risk deafness is partly caused by poor articulation in the language of risk compounded by cognitive overload created by the expectation of individuals to grasp and perfectly execute hundreds of internal policies and procedures. This topic and the research are reviewed in more detail later but these themes are relevant as justification for developing intelligent systems to support security professionals’ efforts to build trust in networked information systems.

“With estimates that at least 95 percent of email traffic in the world consists of spam and phishing, it’s obvious another solution is necessary,” according to Marcus Rogers, director of Purdue’s Cyber Forensics Lab. “Artificial intelligence is among the next steps being considered, combining technology and the human ability to look at information quickly and make a decision.”* Around the same time of the Svpeng attack reported by Kaspersky, an improved version of malware was used to attack Bank of America and other large banks, called Dyre. This variant “found a way to bypass Web encryption, known as secure sockets layer (SSL).”† Reports of Dyre’s use to attack cloud and file-sharing service providers such as Salesforce.com, Dropbox, and Chubby were not verified for purposes of this book; however, if found to be true the implications for AI are obvious. Where does the digital footprint of cybercrime take us from here?

* <https://polytechnic.purdue.edu/profile/rogersmk>

† <http://arstechnica.com/security/2014/09/dyre-malware-branches-out-from-banking-adds-corporate-espionage/>

References

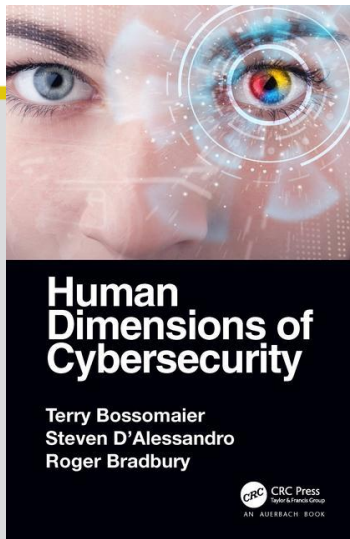
- Burke, L. M., Fueling strategies to optimize performance: Training high or training low? *Scandinavian Journal of Medicine & Science in Sports*, 20. Blackwell Publishing Ltd, 1600-0838.
- Chase, W. G. and Simon, H. A., "Perception in chess," *Cognitive Psychology*, 4, 1973, 55–81.
- Endsley, M. R., Design and evaluation for situation awareness enhancement. *In Proceedings of the Human Factors Society 32 Annual Meeting* (pp. 97–101). Santa Monica, CA: Human Factors and Ergonomic Society, 1988a.
- Endsley, M. R., Situation Awareness Global Assessment Technique (SAGAT). *In Proceedings of the National Aerospace and Electronics Conference* (pp. 789–795). New York: IEEE, 1988b.
- Flach, J. M., "Situation Awareness: Proceed with Caution," *Human Factors* 37(1), 1995, 149–157.
- Goldberg, J. and von Nitzsch, R., Behavioral Finance. Chichester: Wiley. First published in German under the title Behavioral Finance by FinanzBuch Verlag GmbH. Translated from German by Adriana Morris, 2001.
- Kahneman, D. and Tversky, A. (Eds.), *Choices, Values, and Frames*, Cambridge University Press, 2000.
- Klein, G. A. and Salas, E. (Eds.), *Linking Expertise and Naturalistic Decision Making*, Erlbaum, 2001.
- Lerner, J. S. and Tiedens, L. Z., "Portrait of the Angry Decision Maker: How Appraisal Tendencies Shape Anger's Influence on Cognition," *Journal of Behavioral Decision Making (Special Issue on Emotion and Decision Making)* 19, 2006, 115–137.
- Libicki, M. C. and Pfleeger, S. L., "Collecting the Dots: Problem Formulation and Solution Elements," RAND Occasional Paper OP-103-RC, RAND Corporation, Santa Monica, CA, 2004.
- Mack, A. and Rock, I., *Inattentional blindness*. Cambridge, MA: MIT Press, 1998.
- Miller, G. A., "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information," *Psychological Review*, 63, 1956, 81–97.
- Pfleeger, S. L., Predd, J., Hunker, J., and Bulford, C., "Insiders Behaving Badly: Addressing Bad Actors and Their Actions," *IEEE Transactions on Information Forensics and Security* 5(2), March 2010.
- Predd, J., Pfleeger, S. L., Hunker, J., and Bulford, C., "Insiders Behaving Badly," *IEEE Security and Privacy* 6(4), July/August 2008, 66–70.
- Schneier, B., *Semantic Attacks: The Third Wave of Network Attacks*, 2000, <https://www.schneier.com/crypto-gram/archives/2000/1015.html#1>.
- Simons, D. J. and Chabris, C. F., *Gorillas in our Midst: Sustained Inattentional Blindness for Dynamic Events*, Psychology, 1999.
- Simons, D. J. and Jensen, M. S., *Psychonomic Bulletin & Review*, 16(2), 2009, 398–403.



CHAPTER

3

THE FUTURE



This chapter is excerpted from

Human Dimensions of Cybersecurity

by Terry Bossomaier, Steven D'Alessandro, Roger Bradbury

© [2019] Taylor & Francis Group. All rights reserved.



[Learn more](#)

Chapter 8

The Future

In times of peace prepare for war.

Sun Tzu, *The Art of War*

We conclude the book with some guesses as to the immediate future. We consider burgeoning risks, such as security in the internet of things, and the implications they carry for government policy, and the need to consider international actors and nation states. To this end, our recommendations are tailored to specific recommendations for specific types of nation states. We also look at the challenges posed by technologies, such as quantum computing and DNA storage. We also examine the real possibility of a zero day attack and how a coordinated response can prevent or respond to such an event.

8.1 Keeping Nasties Out

We saw earlier in the book that companies, such as Uber (Section 3.4.3.2) and Bose (Section 3.3.3), have been covertly, although not necessarily illegally, vacuuming user data. There is a need for consumers to be sure that an app they download will not be a Trojan horse of this kind.

It is already commonplace for free/open source software to be distributed with certificate keys, enabling the user to determine that the download site is genuine and that the software is what it is supposed to be. However, this does not get around the problem of the software creator adding spyware of some kind.

In the open-source world, it is possible for third parties to read and confirm that software is free of nasties. The mechanisms of distributed trust we discussed will come into play to ensure that these third parties are honest. Thus, although

open source might seem to be cheap and flaky, it can offer extra security through being inspected and checked by lots of people.

Cyber Nugget 49: *Open-source software has the advantage that it can be checked by a lot of people for bugs and hidden nasties.*

For proprietary software, new methods are needed. Legal mechanisms are not likely to be effective. The examples above are probably already illegal in some jurisdictions, but globalization makes any sanctions very hard to enforce. Third party validators are needed. Since organizations entrust confidential data to lawyers and accountants, in principle software source code can be entrusted to a suitably accredited body.

It seems feasible that validators, which have emerged to check open-source software, could morph into accredited entities in the way professional bodies monitor accountants, doctors, and so on. Professional computing societies could act as accrediting bodies. To gain accreditation a validator would need to demonstrate

- Adequate professional expertise. This is commonplace for professional accreditation of higher education courses, and is already something the Association for Computing Machinery (ACM) does across numerous computing and engineering domains.
- Adequate protection of data, presumably encrypted. Already one would assume that lawyers, accountants, and doctors would keep data secure. However, Anthem (Section 3.4.3.2) did not manage to keep patient data secure; hence, the security bar needs to be raised.
- Theft by employees. Rogue employees (Section 2.10) are an ever-present threat to data security as we saw with in Section 2.10. Hardware and authentication systems can reduce the risk of data theft. It is much harder to control the theft of intellectual property, since this may not require anything physical being removed.

On balance, the risk of something going adrift should be acceptable for the assurance that the software is not toxic.

Cyber Nugget 50: *Be wary of apps possibly containing nasties, such as spyware.*

8.1.1 Formal Validation

Some software validators have already appeared, with applications in safety critical areas such as medical imaging. Here the focus is not on keeping out malware,

but on making sure that the software does what it is supposed to do. With electric cars, fly-by-wire aircraft, and other potentially life-endangering systems proliferating, such testing is of paramount importance.

DeepSpec is a consortium aiming at formal software verification. In other activities, formally correct operating systems, such as CertiKOS [124], are under development.

8.2 Use of Encryption

Encryption enables us, in principle, to communicate with other individuals without others being privy to the exchange. In the days of snail mail, countries often had severe penalties for tampering with mail. However, security agencies, where authorized, could open and read any letter. These same agencies now want decryption of electronic communications. A lot of confusion surrounds these issues, particularly with regard to the algorithms. But as Bruce Schneier (Blowfish, etc.) notes, the issues are not cryptographic, so much as human/social/political.¹

Australia has a legal framework, which will give authorities increased access to encrypted communication. At this time, it is also not clear how this will work. Corporations may offer encryption services, which they themselves cannot crack. This became a matter of major news coverage when the FBI asked Apple to unlock a phone associated with the San Bernardino shootings.² Apple refused on the grounds that whether it wanted to or not (and its public position was that it did not want to interfere with the privacy of its users), it simply could not.

There are signs that this may have a negative effect on Australian business. Microsoft president, Brad Smith, said that his customers had in some cases asked to avoid building data centers in Australia. They saw a risk in weakened encryption as a result of these laws.³

The authors concur with the UN position we have already noted (Section 7.15) that the UN regards privacy as a human right and has extended its thinking to the digital age. There is a fine line to tread and it is no time to be apathetic. One is that encryption may become illegal, just as guns are illegal in many countries, except for designated applications. Thus, the encryption of HyperText Transfer Protocol Secure (HTTPS) would be allowed, since it is fundamental to commercial and government activity. But general encryption apps, such as PGP,⁴ or bcrypt (an implementation of Blowfish,⁵ even homegrown encryption), could

¹ www.schneier.com/blog/archives/2018/05/tray_ozzies_encr.html Accessed: 31 May 2019.

² www.theguardian.com/technology/2016/feb/17/apple-challenges-chilling-demand-decrypt-san-bernardino-iphone Accessed: 21 Nov 2018.

³ www.theguardian.com/technology/2019/mar/27/tech-companies-not-comfortable-storing-data-in-australia-microsoft-warns Accessed: 28 Mar 2019.

⁴ www.openpgp.org/ Accessed: 21 Nov 2018.

⁵ www.schneier.com/academic/blowfish/ Accessed: 24 May 2019.

become illegal. We are some way away from this privacy storm as yet and, hopefully, it will remain a black cloud in the horizon.

8.3 Encouraging Good Cyber Practice

Mobile phones, tablets, laptops, home computers, WiFi, cellular data, and almost everybody in the developed world have some form of computer access and much of the rest of the world does too. Facebook is now reported to have over 2 billion users,⁶ over a quarter of the world's population. Many African financial transactions are carried out over mobile phones.

Given such huge computer usage, it is unrealistic to expect most of these people to be anything more than simple users, rather like the many people who slavishly follow recipes, rather than the chefs who invent them. Computer users are still thought of as nerds, albeit sometimes rather wealthy nerds, and not many people have the slightest inclination to dig into the details of how their computing devices work.

The ever-increasing prevalence of cyberattacks of one form or the other means that ignorance and lack of interest are no longer viable choices. Apart from individual risk, one person's risk and cyber compromise may impact on others, say by letting a hacker into a large system.

8.3.1 The Scourge and Salvation of Email

Email is undoubtedly useful. It also has proliferated. Many people, especially if they use email at work, are inundated with messages. Sometimes, messages languish on the server for days, and sometimes, they never get read or attended to. We've seen numerous examples of cyberthreats through email, from phishing to ransomware. Yet email is also a good source of information about cyberthreats, since it is a push service. It arrives on your computer, whether you asked for it or not.

There are numerous good email services for cybersafety alerts. For Example, the Australian government runs *Stay Smart Online*,⁷ a website and regular alert email, such as the December 2018 breach of the Quora forum.⁸ Two problems impede the success of such initiatives: getting people to subscribe in the first place; and making sure that the emails are read or at least scanned for relevance.

Making sure that emails get through depends upon another mild knowledge requirement: effective use of an email client. The more popular email clients

⁶www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
Accessed: 09 Dec 2018.

⁷www.staysmartonline.gov.au/alert-service Accessed: 10 Dec 2018.

⁸www.staysmartonline.gov.au/alert-service/data-breach-public-qa-forum-website-quora Accessed: 10 Dec 2018.

offer ways of automatically sorting emails. Security emails need to be prioritized and spruiked until they have been opened.

Organizations, such as banks, frequently send out security emails (and lots of malware often purports to be from a bank), along with other advertising and general information they send to customers. Thus security emails need to be tagged in some way, although any constant tag could be easily exploited. One possibility might be to integrate a weekly code, sent, say by SMS, with the email header or subject line. Another would be to establish a tag within the email security features discussed in Section 7.13.

8.4 Teaching People Safe Practices

There is a lot going on in this area and even more to do. We just give a couple of examples: gamification in Section 8.4.1 and marketing campaigns in Section 8.4.1.1.

8.4.1 Gamification

One of the exciting developments over the last decade or so has been the use of computer games for teaching and learning [55,123]. Where the material to be taught benefits from simulation, role playing or scenario analysis, games are a natural tool. However, there was also a growing interest in making games out of things, which are not intrinsically game-like. Jane McGonigal [90] describes how she turned domestic chores, such as cleaning the bathroom, into a game with her partner. This is called *gamification*.

There is already gamification activity in teaching good cybersecurity practices. Antiphishing Phil is a game that grew out of research at Carnegie Mellon [125]. As you might expect, it teaches people about how to recognize phishing and believe it or not features fish (Figure 8.1).

Gamification is engaging the few times one encounters it, but it can become tedious thereafter. Partly, this is because the so-called games are not actually very good games. However, there is a lot of scope for development here, since hacker stories have become best sellers — think of the *Girl with the Dragon Tattoo*.⁹

8.4.1.1 Marketing Campaigns for Cybersecurity

Another way of educating people about cybersecurity is to develop social marketing campaigns, which use nudges (Section 4.7). Hayden¹⁰ suggests cybersecurity can be promoted in campaigns which feature

⁹the first of Stieg Larsson's monumental trilogy.

¹⁰Why marketing principles can help a security awareness program succeed (2014). <https://searchsecurity.techtarget.com/tip/Why-marketing-principles-can-help-a-security-awareness-program-succeed> Accessed: 7 Jan 2018.



Figure 8.1: Screenshot from Antiphishing Phil.

- Social currency
- Triggers
- Emotion
- Public
- Practical value
- Stories

Social currency means that cybersecurity issues should be explained in a manner that involves the wider public in what and how to protect themselves and how to respond to data breaches. The information should not be presented as talking down to people, but in a language and style that makes individuals empowered and intelligent. Triggers or cues should be designed in any cybersecurity program so that security is at the top of the mind. Nudges, as discussed in Section 4.7, such as feedback on poor passwords and not using poor security questions, may also serve an important part of this program.

Emotion is important, as emotional content may often be shared. Crafting messages in terms of humor or anger, or even sympathy and compassion may help. An example may be to show the effect on an elderly lady. All cybersecurity

programs should focus on providing tangible cues and evidence of what good practice looks like. This can include rewards for clean-desk policies, having a no piggybacking policy of visitors to the building. In short it is important that cybersecurity policies become apparent and visible in our workplaces and homes.

People are more likely to take onboard messages that have practical value, such as preventing a cyberattack or reducing cyber insurance premiums. It also suggested that incentives may be used to encourage cybersecurity, such as providing software to encrypt hard drives that may benefit both the user and the company.

Stories are important because lessons or morality about cybersecurity can be shared online. Police-type lessons do not work well, as opposed to a focus on characters and the humor involved in sometimes unpleasant situations of cyber breaches. Simply put content that is fun and engaging is more likely to be shared and discussed at home and in the office. What these hallmarks of good cybersecurity communication show is that it is not the amount of information that is important, but the nature of communication and how this information about cybersecurity is communicated to different groups or niches in society.

8.5 Changing Criminal Models and the Arms Race with the Authorities

It is possible that criminal and hostile states are more organized than those who seek to protect our cybersecurity. As noted in Chapter 5, the threats faced by all of us are constantly evolving both in technology, vector of attack, but more importantly by the business model criminals and hostile states wish to use. Examples are the use of ransomware, business email compromises, threats of denial of service, and the stealing of IP by criminal insiders, and members of hostile states. The use of social engineering also shows that cybercriminals can adapt quickly to the frailty of human behavior to get around security design and technology. A worrying trend is the use of criminal networks such as the Necrus group by hostile states as privateers to steal information and/or disrupt the infrastructure of opposition countries. For many in the population, this means that keeping up to date with the intelligence of threats and how to avoid them is vital.

It should be noted that reactions to cyberattacks and threats are fragmentary and depend on cooperation across different jurisdictions with different legal and regulatory frameworks. Also many technologies and systems used to prevent attacks are not coordinated to provide overall enterprise security. A good example is the use of cloud technology to store critical data. As noted in Chapter 6, this is seen as an out-of-sight out-of-mind solution of contracting out security of vital assets to a third party. On the other hand, those who seek to disrupt, steal, threaten, and even destroy our security are better organized through criminal networks working with hostile states, where intelligence and knowhow on how to

conduct cyberattacks is easily shared. As noted also in Chapter 6, the costs and expertise now to engage in cybercrime are minimal, or can be provided on a percentage of return basis. We are therefore likely to see cyberattacks becoming more common with small and medium businesses, and more individuals as barriers reduce entry of criminals, while the competition to provide services increases.

8.5.1 Do People Learn?

Despite media reports of massive breaches, popular fiction of cyberthreats in films like *Die-Hard 4.0* or in television series such as *Mr Robot*, it seems that human behavior in cybersecurity is difficult to change, even for those who work in national security or in technology companies. In a recent report by security company Dashlane, Katz noted in 2018¹¹

- The Government Accountability Office (GAO) in the United States government was able to guess Admin passwords in the Pentagon in just 9 seconds, as well as discovering that passwords for multiple weapon's systems were protected by default passwords, that any member of the public could find online.
- The state of Texas left 14 million electoral records exposed on a server that was not password protected.
- There are around 1 million corporate email and password combinations of top UK law firm available in the Dark Web. Most of the credentials stolen were in plain text.
- An Indian engineering student hacked into one of Google's pages to access a TV broadcast satellite. The student logged in using his mobile device on the Google Admin pages with a blank username and password.
- A White house staffer allegedly wrote down his email login and password on White house stationary, which he then left accidentally at a DC bus stop.

No technology can really protect us from our carelessness. The examples all show the problem of having only one weak link in security can cause serious breaches. Organizations and individuals need to see cybersecurity as fundamental risk and not just an IT issue. Governance, training, and monitoring of people with access to important information is also the most perplexing but important issue for the 21st-century political economy.

¹¹Kanye West Tops Dashlane's List of 2018's "Worst Password Offenders" https://blog.dashlane.com/password-offenders-2018/?utm_source=email&utm_medium=appboy&utm_campaign=19774335-05fd-4bb8-bb48-9e2d05587b38&utm_content=1&utm_term=en&utm_type=news Accessed: 20 Dec 2018.

8.5.2 New Legal Agendas

We have seen a number of examples of where vendors have sought to exploit information in a deceptive way. Bose (Section 3.3.3) used their control app for harvesting musical activity. Superfish and PrivDog hijacked HTTPS security (Section 2.9). Such vendors may have already obtained permission to do this when the user agreed to the terms and conditions.

Lengthy legal contracts are a fact of life in the cyberworld, and most users have little option but to agree. Thus, entry to the Apple store *for any app* requires a blanket agreement. The GDPR helps a little with this, but we believe that terms and conditions should be legally required to state in everyday language right at the beginning, an executive summary if you will, a number of important conditions, such as

- Whether the app harvests data to onsell to other vendors. Some companies, we have seen earlier in the book, have been less than perfect in this regard. **It should be clearly stated what information an app harvests and whether it onells it.**
- Whether the app interferes with security protocols such as HTTPS.
- Whether personal data can (a) be exported in a universal, nonproprietary format and (b) how personal data can be completely expunged, including backups, log files, clipboards, and innards of algorithms.

As this book goes to press, Bloomberg reported that Amazon has huge teams of people listening to Alexa,¹² its home assistant.¹³

In a response to the story, Amazon confirmed to CNN Business that it hires people to listen to what customers say to Alexa. But Amazon said it takes “security and privacy of our customers’ personal information seriously.” The company said it only annotates an “extremely small number of interactions from a random set of customers.”

The situation is slightly less sinister for Apple, again according to Bloomberg,¹⁴ its home assistant¹⁵

¹²www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio Accessed: 13 Apr 2019.

¹³<https://edition.cnn.com/2019/04/11/tech/amazon-alexa-listening/index.html> Accessed: 13 Apr 2019.

¹⁴www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio Accessed: 13 Apr 2019.

¹⁵<https://edition.cnn.com/2019/04/11/tech/amazon-alexa-listening/index.html> Accessed: 13 Apr 2019.

Apple's Siri also has human helpers, who work to gauge whether the digital assistant's interpretation of requests lines up with what the person said. The recordings they review lack personally identifiable information and are stored for six months tied to a random identifier.

8.6 Hyperstorage and Machine Learning and Privacy

Facebook went under intense scrutiny following the apparently illicit use of over 50 million user's personal data by firm Cambridge Analytica. The information was used to generate personal ad campaigns in the 2016 US presidential election (Section 2.8). The threat, and possible benefit, from machine learning is increased manyfold by the ease of storage of extremely large volumes of data, what we call hyperstorage. Data storage costs energy, thus new storage technologies with much higher information density and lower energy costs could be transformative. One such technology is DNA storage—using the DNA molecule itself as a storage medium (as opposed to it storing a genetic code). It has already been demonstrated, but currently costs around \$3K/MB and thus needs to come down in price significantly.

The significance of hyperstorage combined with rapid progress in machine learning means that very little online information will remain secret. For example, telcos could record every single phone call, convert it to text and search it for anything, from advertising opportunities to criminal intent. To see how easy this is, imagine you spend 2 h everyday on the phone at 64 Kbps (a decent MP3 rate), which would amount to about 20 MB. Thus, 10 years of calls would equate to 200 GB. Peanuts. Hence, the need for increase privacy.

8.6.1 Protecting the Vulnerable from Themselves

It could also be argued that the threats of cyberattacks, beyond those of carelessness, are too complex and dynamic for many in society to deal with. Examples may be the elderly, less educated, and small businesses who lack the infrastructure and resources to be able to defend or rebuild after an attack. Designing in security for a society may therefore become an important option. This could include the use routers that monitor individual WiFi hotspots for homes and business that report suspicious behavior, provide greater security and guidance on stronger passwords, have built-in password safes and VPN capabilities. These routers could also have reminders on updates on operating systems. These systems could be produced at low cost and become mandated or distributed by government to vulnerable consumers. Of course technology cannot protect us from our own carelessness and lack of forethought, or new social engineering risks, but it can at least like a burglar alarm make a cybercrime less likely.

8.7 The Mink and the Porcupine

Porcupine defends herself from predators with her sharp spines, difficult to strike or bite. You need kevlar gloves to pick up a porcupine. Mink on the other hand has a beautiful soft coat, but he is a voracious predator with very sharp teeth. You need kevlar gloves to pick up an angry mink too.

Most of the cybersecurity measures discussed in this book are porcupine defenses, making it as difficult as possible to get in. At the state level, cyber warfare is starting to emerge as a national strategy, although Stuxnet was very likely an example of a state attack. Thus, mink-like strategies of hunt and kill are increasingly prevalent at this level, but much less so at a corporate or home level.

We began the book with the story of the first computer virus, Creeper, and Reaper, a cyber mink sent out to destroy it. Perhaps we need legal and accreditation frameworks for more attack software. Why wait for a network of unsecured Internet of Things (IoT) devices to become a botnet for a Distributed Denial of Service (DDoS)? Why not be more proactive and search out and get their owners to secure them in some way. We need more cyber minks.

There are some powerful tools already out there. Marcin Kleczynski found *Malwarebytes* after picking up a nasty virus in 2004. Now a company with over 700 people,¹⁶ it develops tools for hunting and destroying malware, beyond the usual antiviral software.

Another mink comes, Falcon OverWatch, from CrowdStrike¹⁷ that searches out threats of all kinds, known and unknown, in real time.

8.8 Take It Away, Renatus

The message of this book is that good cybersecurity depends on people as much as, or even more than, technology. We have seen how destructive and costly a cyberattack can be, from ransomware to fake news. When computers have been set up and configured, there is a strong urge to leave well alone. This is not irrational. An operating system upgrade can sometimes break existing software, perhaps with very high cost. However, we believe that good cyber hygiene to avoid attacks pays off in the long run. Deception, such as email spoofing, and false assumptions—nobody could possibly know my mother’s maiden name—lead us into trouble. Thus, we give the last word to Roman writer Publius Flavius Vegetius Renatus, a millennium and a half ago, often wrongly attributed to Sun Tzu in the *Art of War*

Si vis pacem, para bellum. *If you want peace, prepare for war*

¹⁶www.malwarebytes.com/company/ Accessed: 12 Mar 2019.

¹⁷www.crowdstrike.com/why-crowdstrike/ Accessed: 12 Mar 2019.