APPLIED RESEARCH LAB FOR INTELLIGENCE AND SECURITY

START NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

Countering Insider Threat (CInT) Simulation

September 30, 2021

Ron Capps[1]* and Devin Ellis[1]*
[1]National Consortium for the Study of Terrorism and Responses to Terrorism
*corresponding authors, rcapps@umd.edu and ellisd@umd.edu

Created by:

The ICONS Project

The Applied Research Lab for Intelligence and Security (ARLIS) is The University Affiliated Research Center (UARC) for Sociotechnical Systems and Advantage in the Human Domain at the University of Maryland

ARLIS
7005 52nd Avenue
College Park, Maryland

EXECUTIVE SUMMARY

As part of ARLIS' work to support the Department of Defense through the Countering Insider Threat program, the University of Maryland's ICONS Project was funded to develop and implement an online training exercise. The materials presented here are the content of that exercise which can function as a stand-alone, in-person tabletop, or can be conducted over the ICONSnet online platform for distributed use.

The design of the exercise sees participants taking the roles of five key C-Suite executives (or their teams) at a fictional defense contractor, Kings Bay. All names and characters in the scenario are fictional. As the exercise unfolds, they are presented with a series of vignettes that highlight the challenges of dealing with different types of insider threats. A defense contractor was selected as the base for the scenario because of its connectivity to the various stages of work on programs that present differing profiles for insider threats: basic research, classified R&D, production, an interface/embedding directly with the government.

Each of the vignettes that the participants receive focuses on a slightly different dilemma, ranging from potential espionage to information exposed due to human error, to the potential for workplace violence. For each, the differing C-Suite executives have their own individual goals and objectives based on their functions within the corporation - but also must have the wellbeing of the company, the employees, and the national security firmly in mind. Their objective is to propose a course of action to mitigate or resolve the issues raised in each vignette and present them to the facilitator. The learning objective is not to get a 'correct' answer to each dilemma - in some cases there might be multiple good solutions, or none. The objective, rather is to think more about how to tackle the hard problems in this space, and have an opportunity to learn through review and debriefing of the decisions they make.

Contents

Insider Threat Simulation

As a capstone exercise for this class, we will take part in a simulation that will allow you to exercise some of the things you've learned in the course. The simulation will take place over four 90-minute class periods. The first three periods will be rounds 1-3 of the simulation itself. The fourth period will be for discussion and review with the course instructors.

The simulation is set at HRG, Inc., a fictional global defense contractor. The action takes place at HRG's facility in Georgia near the U.S. Naval Station Kings Bay. This facility is involved in research and development of technology for use aboard U.S. Navy submarines.

During the simulation you will take on the role of a member of the senior leadership team of HRG-Kings Bay. All names and characters in the scenario are fictional. Each of the individuals (chief of staff, director of security, information technology chief, human resources chief, director of research and development) carries equal weight in the organization. You should work for the good of the organization, but also as much as possible, to protect your staff and their work.

Background

You work for HRG, Inc., a global defense contractor. HRG develops and produces technology that the U.S. and other militaries use for C4I (command, control, communication, computers, and intelligence) and ISR (intelligence, surveillance, and reconnaissance). These products include satellite communication systems, GPS systems, radar and sonar, unmanned aerial vehicles, and so on. The research and development programs at HRG-Kings Bay (HRG-KB) are primarily devoted to submarine communications and other highly sensitive technology. Many of these research programs are classified at the Top Secret (TS) level and require access to Sensitive Compartmented Information (SCI).

HRG's global headquarters (HRG-HQ) is in Reston, VA. HRG's senior leadership grants significant hegemony to research center leadership, and thus each of the outlying facilities (like HRG-KB) are semi-autonomous corporate fiefdoms. The leaders of the facilities are responsible for the successes and failures of their teams, and for everything that happens or doesn't happen under their leadership. HRG-KB's work culture is rigidly hierarchical. The senior leaders here expect a certain amount of deference. Once they have made a decision, leaders expect their instructions to be carried out, not questioned. While they claim to have open door policies, quite often the C-Suite executives are cloistered, sheltered and protected in their offices by mandarin gate-keepers.

But, HRG-KB isn't alone in conducting this research; the research and development team has partner organizations who carry out elements of research in which they are the acknowledged subject matter experts or because they have specialized equipment or capabilities. And while these partners are external to the organization, their involvement with the R&D section means that every other section, from security to IT to HR to the C-Suite, interacts with them in one way or another. (For more information on these partner organizations, see below.) Because of the nature of the work HRG and its partners are conducting, HRG-KB policies and procedures must apply to all team members, regardless of their location or affiliation. This sometimes leads to friction between HRG-KB leadership and the private sector and academic researchers.

Partner Organizations:

SARGO

A private corporation created and led by Amy Preieto Sargo, Ph.D. Dr. Sargo holds numerous U.S. patents related to digital communication frequency adaptability. She recently took her corporation public, raising more than $700M with the initial public offering—mostly from venture capital hedge funds. The corporation invested the windfall in the purchase of tech firms (one in Israel, the other in China) engaged in R&D that supports SARGO (and in some cases, HRG-KB). SARGO's headquarters is on the Kitsap Peninsula in Washington. Dr. Sargo's work on orthogonal frequency-division multiplexing is of interest to HRG-KB's research and development team.

Maritime Technology Institute (MTI)

Located in Kittery, Maine, MTI is a private university with undergraduate programs principally focused on training maritime/naval engineers and scientists, some of whom go on to serve as Merchant Marine, Navy, or Coast Guard officers. MTI's graduate programs (MS, MEng, and Ph.D.) include several engineering fields, physics, materials sciences, and oceanography. MTI also has a research facility that is wholly funded by private research grants, some of which come from the U.S. government and some from foreign entities. Of interest to HRG-KB is MTI's work with ELF (extra low frequency) and VLF (very low frequency) communications.

Competitors:

Consolidated Systems

HRG's fiercest competitor, Consolidated, is as deeply engaged in every military technology market as HRG. At home, the Defense Department procurement officials, Congress, and the administration all play off of this competition to drive research and development. Globally, near peer and other nations benefit from the competition as well; with multiple options for most every type of technology they might need, they can shop around. Consolidated's home office is a short Metro ride away from HRG's. Their submarine technology research facility is located in Groton, C

Day/Round 1

You're in your office at HRG-Kings Bay. Read your messages first, and then go to the resources section and read your assigned role sheet.

1. News Report: The New York Herald.

Los Angeles. FBI agents detained two men trying to board a flight out of Los Angeles' LAX airport bound for Singapore last night. No personal information about the men detained was available. A.M. Curry, special agent in charge of the FBI's Los Angeles field office said in a brief statement that, "the two men were involved in a breach of highly classified military research and development information."

2. Email.
From CEO
To: HR, Security, R&D, IT, CoS.

> *As you've all probably heard, Consolidated Systems has had a major, highly-classified defense research project compromised. The initial reports point to some sort of insider attack. Given the similarities in our research, I'm concerned that we may be next, if we've not already been hit. Please meet in the executive conference room this afternoon to discuss our strategy moving forward. Bring ideas for continuing our important work in the most secure way possible and report to me your recommendations. —Signed, The CEO.*

Role Sheets

Security

You're the security manager for HRG's Kings Bay research center. You manage a team of professionals who cover work ranging from information systems security and personal security clearances, to physical security and even badging of staff. Generally, your day-to-day work is pretty mundane, because you've already done the groundwork. This leak or theft of information from Consolidated Systems could be serious. If the same thing happened here, you'd be out the door in a flash and probably never work in this business again—to say nothing of the potential security risk to the defense of the nation.

One of the biggest challenges for any security officer is to balance security against operations. It's actually very easy to keep something completely secure: lock it up and don't let anyone play with it. But it's harder to keep things secure if others have access to them and they can be brought out of the safe and handled. Your challenge is that this corporation is in business to create new technology and apply it to the defense of the nation. In order to do that, people have to have access to secret stuff. And more often than not, it's the people who are the weak link in the security chain.

Your approach in these discussions should always lean toward solutions that are more secure without being ridiculously restrictive. Be reasonable but get as much as you can.

Information Systems

You oversee the computer systems team for HRG's Kings Bay facility. There are more than 500 separate computers within the facility. Everyone has an unclassified system and anyone with a clearance has one or two classified systems on their desk. All of this technology has to be kept secure if you are to stay in compliance with the Defense Department's systems security regulations. You've got a good system going. The R&D computers operate on their own network that isn't linked to the outside world—you've set up an air gap between them and the everyday work computers for emails and such.

This failure at Consolidated Systems had to be a human error, right? I mean no one would be dumb enough to allow their systems to be compromised, would they? Well, there was that Stuxnet thing, but that's different—or is it?

Part of the problem with system security at HRG-Kings Bay is the variations in type of desktop systems. The people in R&D rightly have top of the line desktops. But the folks in admin, HR, and other less technical workplaces have cheaper, less-advanced (and thus less secure) desktops. Those computers have CD and USB ports. It would be incredibly easy for anyone to access the system, download information onto a CD-RW or flash drive and, well you don't even want to think about that.

In these discussions, you should focus your efforts on technological fixes. Push for acquiring the most secure systems and software available. Point out the dangers of keeping the old systems and the potential for unauthorized capture and transfer of data. Push to use technology in ways that improve security throughout the enterprise. In this way you can increase your value to the company while demonstrating the importance of the proper exploitation of technology.

Human Resources

You're the director of human resources for HRG-Kings Bay. You're in charge of the hiring and firing but you're also the training manager, you keep an eye on compensation and benefits, you protect employees' rights under the various state and federal laws, and you also direct the internal and external communications teams here at HRG-KB. The breakdown over at Consolidated Systems might have been an inside job, either intentionally or not. Or, it might have been conducted from a computer farm in North Korea. But if there is an insider threat here, you want to solve this quickly and quietly.

During these meetings you should focus on and be open to new procedures and policies that will clearly improve security throughout HRG-Kings Bay. For example, you might propose an improved, mandatory on-boarding process that includes briefings and tests on security standards and protocols. But you should also be aware of policies or requirements that run counter to accepted HR norms in personal privacy or seem likely to lower morale in the company. You have research partners in academia who cannot comply with certain restrictions—they might not have secure compartmented information facilities or SCIFs, for example—and it's your role to watch out for their interests as well.

Research & Development

You're the director of research for HRG at Kings Bay. You're a research scientist and you've assembled a first-rate team of scientists and technicians to take on a huge technical challenge. Among the team are physicists, chemists, maritime engineers, oceanographers, marine biologists, metallurgists, and more. This tasking from the CEO is keeping you away from your work. Do your best to get through this as quickly as possible so you can get back to work.

Most of the most secret information at HRG-Kings Bay is in your area. Your researchers and number crunchers have the materials and the data that is the core purpose of this organization. You also collaborate with outside researchers, some of whom are in academia and some are in the private sector. These partners conduct research that is remarkably similar—and in some cases identical—to yours, except that it isn't classified. It seems it's a question of end users and intentions. Your end user is the U.S. Navy and the Navy's intention is to make better submarines to better protect the nation. The partners' intentions are to make better technology to do things like fight climate change. Your research is classified; theirs is not. You would very much like to make all of this work unclassified. During these meetings you should push for the least restrictive policies and systems.

Chief of Staff

You are a member of the C-Suite team at HRG-Kings Bay, Inc. The CEO has assigned you to this task force to make sure that this potential security issue doesn't get in the way of the real work. After all, just because one of your competitors has been hit, doesn't mean you will be, right? Maybe the other guys were lax in their security protocols. Still, maybe an adversary nation captured Consolidated Systems' data by specifically targeting them in response to a high-priority intelligence requirement. Maybe something that Consolidated was working on was particularly of interest to the bad guys. Wouldn't that mean you were also a likely target?

Within the task force you have the authority to kick off the meetings but the directors who make up the rest of the task force are your peers. You can't ignore their concerns or give them orders. You all work for the CEO. Your job in all of this is to represent the C-Suite—the leadership of this organization— who are responsible to HRG-HQ and to the stockholders. You're mostly interested in getting on with the work via the quickest and least disruptive methods necessary.

Instructions:

Step 1. Using the knowledge and insights you have gained in this class, think about what the organization should be doing to protect itself from insider threats. Individually, and acting in your assigned role, make a list of proposed actions and policies. Then go to Step 2.

Step 2. As a group, share your individual recommendations and, from those, develop a set of recommendations to send to the CEO. You might consider creating them under headings like personnel, information security, technology, training, physical security, corporate culture, and others. Your recommendations don't need to be fully developed. Just offer the basic idea of what you're recommending and why you think it's worthwhile. What sort of risk or vulnerability is it supposed to counter? For example: If you choose to require identity badges you don't need to worry about what shape or color they are, simply note that you want to have them and why (they should serve a specific purpose like denoting a specific level of security clearance and thus afford access to secure areas). You should include a short paragraph with each of the major points detailing what the problem or threat you're addressing is and why you want to implement that specific element of the strategy.

Reporting your results to the CEO marks the end of Round 1.

Day/Round 2

Email
From: CEO
To: Ad Hoc Security Working Group
Subject: Your proposals.

Good work, everyone. Thank you for your efforts. Here's what I'd like to do. I want this team to become an ad hoc working group that will meet regularly to discuss our security. I have accepted several of the proposals put forward by the group and added a few of my own to create a comprehensive security policy. I think it's pretty good, but I'd like you to go over each element and let me know what you think. Is it sufficient? What are we missing? What will the effect of these changes be on our productivity and creativity?

—HRG-KB will immediately enforce restrictions on personal electronic devices in the workplace. No personal electronic devices (smartphones, cell phones, smartwatches, mp3 players, etc.), data capture devices (CD-RW, flash drives, cameras, etc.), or wearable technology (fitbit, GoPro, earbuds, Google Glass, etc.) will be allowed on the grounds of the HRG-KB campus or in any HRG-KB buildings (excluding the core of the C-suite area).

—The information technology team will immediately disable all external ports for USB, CD, or other data transfer systems, all sound cards, and private internet access capability on all HRG-KB and remote partner computers.

—Identification badges with images of the authorized wearer and immediately recognizable, color-coded area access markings will be required immediately. These badges will be used to "badge in" and "badge out" of secure areas and, regardless of the wearer's assigned workstation, must be worn and visible at all times when on the HRG-KB campus.

—Non-C-Suite staff will provide all of their social media (Facebook, Twitter, Instagram, etc.) handles and site URLs, plus lists of any civil groups, clubs, and other organizational memberships they hold to the security and HR sections. The director of security will delegate a

security team member to monitor and scrutinize all staff personal social media. The director of human resources will delegate a team member to monitor and scrutinize all staff outside organization memberships.

—Classified documents and data must be secured in a Class 5 security container when not actively in use. Classified information may not be simply "lying about" on employee's desks or computer screens where it can be misused; there is no open storage at HRG-KB. If you aren't actively working on a document or actively engaged with your classified computer system, put the document back into its proper file in the safe or disengage your classified hard drive and put it away. Don't forget to spin the dial! An unlocked safe is an invitation to espionage.

—Computer systems will be compatible and consistent with the security level of the area in which they are placed. For example, within the SCIF, only those computers authorized to operate using TS/SCI material (and authorized to operate on the JWICS Top Secret network) will be allowed. Any computers set for Secret (and set up for the SIPRNet) or for Unclassified (NIPRNet) information will be set up outside of the SCIF and users must exit the SCIF to access these systems. Computers carrying classified research data that is proprietary to HRG (and caveated PROPIN) will not be linked to any outside network.

—Security will install security cameras and audio monitoring microphones in every workspace, hallway, public space, and across the exterior campus. These systems will be programmed to record and maintain (for a period of 90 days) images and audio of everything that happens within their assigned range. Security will review this data weekly for anomalous activities.

—"See Something, Say Something" anonymous reporting boxes will be placed in each lunchroom, breakroom, at or near each entry/exit point, and outside the C-Suite offices. Staff will be encouraged to anonymously report any anomalous activities. Further, security will adopt an affirmative open reporting policy for all employees (perhaps known as the Security Team Staff Access Initiative or STASI). Any employee who has security concerns about another employee should report those concerns directly to the chief or deputy chief security officer.

> *—All HRG-KB personnel will be required to attend mandatory, monthly security training events organized and implemented by the security and HR departments. This includes all remote and partner staff. Each training session will conclude with an examination on the security policies and procedures at HRG-KB. All non-C-Suite employees will be required to pass these examinations with a grade of 90% or higher.*
>
> *—HRG-KB will adopt a "Zero Tolerance" policy on security infractions. Any non-C-Suite employee found to be in violation of any of these policies will be subject to termination. One strike and you're out!*

Instructions: Working as a group, and again acting within your assigned roles, consider each of the elements in the CEO's proposed security policy outline. Determine where the policy is sound and where it isn't. By the end of this class period you should submit a response to this outline detailing any problems and proposing better solutions. If you cannot come to a consensus among the group, that's OK. But make sure each member's opinions and suggestions are represented in your document.

Reporting your results to the CEO marks the end of Round 2.

Round 3

NOTE: *Entering the third class session, instructors determine how they intend to manage the fourth and final class session. There are nine vignettes presented in session three that the students will discuss. For session four, the instructors have nine potential 'results of investigation' to work with. The instructors can use these in their final class session or create their own. The provided scenario results point to the limits of continuous evaluation, false allegations, ambiguity, carelessness, and several actual, serious threats. These can serve as a lead-in for a post-course review and discussion.*

Several months have passed. Not long after the former CEO sent you the draft security policy, HRG's management in Herndon, VA, instituted what they called "the new way forward." This is a program designed to break down hierarchical structures, reduce bureaucracy, and introduce a more horizontal management structure. The program has shown promise, with mid-level managers having more of a voice in program design and implementation. Workers across the enterprise seem to appreciate the leveling effect this has had on the workplace.

Mid-level managers are encouraged to visit other team offices or buildings to get an idea of what the other parts of the organization are doing and how. C-Suite executives join staffers in the breakrooms and regularly appear in the hallways taking part in what the new CEO calls "management by walking around." This has occasionally resulted in improved performance in some processes when a director gets a straight answer from a technician.

This month's security meeting has been dedicated to discussing a few individual cases that have been brought forward or otherwise come to the attention of the committee. During the meeting, discuss each individual case and consider what is HRG-KB's risk or vulnerability, then determine what you think needs to be done about it.

Instructions: By the end of this class session the group should develop a document with your recommendation (just a sentence or two) on how to proceed with each individual case study. Try to answer these questions: What is/are HRG's vulnerability? What is the risk? What should HRG do? If you cannot come to a single agreed-upon approach, that's OK. But make sure everyone's recommendations are represented in the document.

Case studies for Round 3.

Offhand comment.

Recently, an offhand comment by one of the admin section's contractors raised issues about a change in activity in the C-Suite. The contractor, a technology maintenance and repair technician, commented that one of the four copiers in the C-Suite support office had been busier than normal. That copier had only a slightly higher count of jobs sent to it, but some of those jobs were demonstrably larger than others, including one that was for more than 200 pages. Generally, any job requiring more than 50 pages or so would be sent to the print shop or farmed out to an outside printer. The admin staff in the C-Suite handle every sort of information that goes through the office including government classified documents and corporate proprietary information. Looking at the digital user logs, those jobs were all run by Terri McKinney, one of several admins who support the C-Suite. Terri has been with the organization for many years. She is widely thought of as nice enough, but a little odd, gusting batty. What should we do about this?

Anonymous Tip.

This handwritten note was in the "See Something, Say Something" box outside the lunchroom: "Somebody ought to take a look at KC Bryan. Last week I saw a pile of classified documents, data sheets or something, and an envelope stuffed with cash on KC's desk. And I know KC isn't supposed to have access to that stuff. Something's wrong here." What should we do about this?

Accepted Practice.

Last week, while one of the C-Suite types was managing by walking around, they noticed that an employee had an iPod on their desk inside the SCIF (secure compartmented information facility), the most secure part of the building. Flash drives, mp3 players, smartphones, or any other type of data storage devices are unauthorized in the secure areas of the buildings. Employees are provided with storage boxes outside these areas where they are expected to deposit their devices before entering the secure area.

When asked, the employee said, "Look, everyone here does it. We can't concentrate with all of the chatter going on in this open plan office. So we bring in iPods to listen to music through noise cancelling headphones. It's the only way we can get our work done." In fact, the employee is right. Many employees use headphones to stream music off of their devices, even while in the SCIF. No one bothers to say anything because it's an accepted practice, and no one inspects the area or employees' bags when they are entering or leaving the office or the SCIF. Is there a problem? If so, what should we do?

Concerned Co-Worker.

A mid-level shift leader, Karyn Crosby, last week filed a note with security about another employee, Matthew Spady. Karyn and Matthew work in the same open-plan space at HRG-KB. Karyn said that Matthew's behavior around the office had changed noticeably in the past few weeks. He's been coming in early on some days, coming in late on others, staying late some nights and leaving early on others. She said Matt had recently bought a vintage Corvette and, as Karyn was walking past Matt's desk the other day, she saw he was surfing 'yachts for sale' sites on the web. She thinks this is a problem. Is it? What should we do about this?

The Problem with Partners 1

Soraya Verjee, one of the lead researchers on a Maritime Technological Institute (MTI) program with HRG-KB has published a peer-reviewed paper on one aspect of the technology she is developing at MTI. The thing is, the element of her unclassified research she's writing about is also part of the classified technology she is developing with HGR-KB. She posted on her personal Twitter account (on which she is identified as a senior researcher at MTI) that all technology should be open source to allow more nations access to it as a way of addressing issues like climate change, loss of biodiversity, and other global environmental challenges. Is this a problem? What do we do?

The Problem with Partners 2

Earlier this year, Dr Amy Preieto Sargo used a windfall of hundreds of millions of dollars to acquire two foreign-based research firms, one in China and one in Israel. This week, the Wall Street Journal reported that SARGO, Inc had begun transferring some of its research into orthogonal frequency-division multiplexing to the Israeli office. The technology itself isn't classified, but its use by the U.S. Department of Defense is in some cases. The research that SARGO is doing with HRG-KB certainly is. Is this a problem? What do we do?

Culture Clash

A routine scan by the information security office showed that a new employee, Wang Li, had used a flash drive to access files on one of her classified computers. This is unauthorized. The same flash drive had also been used on her unclassified computers, one that is connected to the open internet. This is authorized on unclassified computers, but Ms. Wang works in the SCIF where flash drives, mp3 players, smartphones, or any other type of data storage or transfer devices are unauthorized. Employees are provided with storage boxes outside these areas where they are expected to deposit their devices before entering. Li is a new employee working on some of HRG-KB's most highly sensitive programs. She is a naturalized citizen who was born in the People's Republic of China. Her parents remain in PRC while they await decisions on their U.S. family reunification immigrant visa applications. What should we do about this?

Clicks

A team member has been behaving oddly for some time. CJ Finerty is a senior chemist in the R&D section. A few months ago, CJ and his spouse split up. This was pretty surprising because the two had seemed quite happy and comfortable together. In the past months, co-workers have noticed CJ taking a lot of breaks from his desk to check his phone. CJ's boss even made a joke about it and CJ got a little upset. He asked if there was some policy against checking his Twitter feed. The boss got curious and looked at CJ's Twitter feed just to see what was so interesting. (It's not a locked account.) For months now, CJ has been Tweeting about government surveillance, suppression of fundamental freedoms, Martial Law, the "Deep State," and the military-industrial complex. Some of CJ's Tweets reference conspiracy theories like Chemtrails, the Illuminati, the Joplin Tornado, and Bilderbergers. Plus, there are lots of pics of CJ showing off his massive collection of weapons. The tone of these Tweets has gotten more and more strident over the past weeks and CJ's boss is concerned. Is this a problem? If so, what do we do?

Save the Whales

For several months now, protestors have appeared at the entrance of HRG-Kings Bay and near the facility's working dock in boats attempting to disrupt research and testing. Protests against defense contractors or facilities aren't terribly unusual, but the timing of these protests is interesting. Every time HRG-Kings Bay has used its research vessel to carry out testing of some piece of technology, the protestors have appeared.

The protestors claim to represent a loosely-organized collective of animal rights groups called PAAR (Protecting All Animal Rights) and here in the Kings Bay area they are focused on the damage U.S. submarine operations can do to marine life, particularly whales. HRG-HQ sent a team of videographers and analysts down to Kings Bay to film the protests. Here's what the analysts found: (1). The protestors come in two groups (at the front gate and on the water) in order to challenge HRG-Kings Bay physical security systems and to garner more public scrutiny of HRG-Kings Bay activities; (2) The protestors clearly know when the research vessel will sail on testing operations. They do not attempt to disrupt non-test-related movement by the vessel (such as maintenance or fueling trips); and (3) The protestors film the activities of the boat crew, the researchers aboard the boat, and the on-shore security personnel. The videos could be used to learn the identities of HRG-Kings Bay team members, to understand HRG-Kings Bay and local police security procedures and tactics, and/or to feature in fund raising or other video presentations by the group.

It's clear the protestors have an inside source for information. There are three HRG-Kings Bay staffers who might be involved with the protestors as a source of information (or worse).

- —Mary-Margaret Daughtry. Mary-Margaret works in the R&D section as a technician. She is an animal lover and rights advocate. She is a vegan who rides her bike to work and has crystals and a dream catcher hanging on the walls of her cubicle. Last year she went on a cruise to Antarctica during which she took part in the annual penguin census. She is, as well, a first-rate and highly respected technical crew member/data scientist. Her principal specialty is data capture and management during field testing. She is always aboard the research vessel when it sails and would certainly know when tests were planned.

—Kristi Penn. Kristi is the research vessel's captain. After graduating from the SUNY Maritime College with a degree in marine environmental science, Kristi had a career in the Merchant Marine. After her service, and despite being offered jobs captaining massive cargo ships travelling around the globe, she chose to take the job with HRG-Kings Bay captaining a 76' former longline trawler that HRG-KB transformed into a modern offshore research vessel. Kristi is a serious environmentalist who, in her spare time, is studying for a doctorate in environmental science (she sometimes does a little data collection of her own on the trips out to support her Ph.D. research). The HRG research vessel doesn't move without Kristi, and she takes part in discussions of research objectives with the scientists so that she can best direct the boat to their needs.

—Martin Green. Martin is HRG-Kings Bay's resident marine biologist. It is his job to consider the effects of all research and of the potential effects of end user technology on marine life. Martin came to HRG-Kings Bay from the Woods Hole Oceanographic Institute where he directed the institute's long-term, large marine mammal migration program. Martin is married to a documentary filmmaker whose film about the water crisis in Flint, Michigan won a prestigious award. Martin is privy to every research project and takes part in all at-sea research.ou

Is this a problem? What do we do now?

Round 4

NOTE: *During the fourth and final work period, instructors may choose to provide feedback on each individual case study. Listed below are potential outcomes.*

Offhand comment.

Terri is taking advantage of the company's policy that it's OK to use company assets like copiers and fax machines for occasional, small jobs, or to raid the office supplies the week before your kid starts school. In Terri's case, she's been printing fliers for her grand-daughter's middle school class presidency bid.

Anonymous Tip.

KC runs the office NCAA March Madness pool. The documents seen on the desk were entries submitted by other employees and the envelope contained their entry fees. The documents and the information contained on the pages themselves weren't classified, but two of the pages were printed on colored paper that should only be used for classified documents. The staff member who printed their entry was working on a computer in their workspace and accidentally printed to the drawer (filled with a specific color paper) that is used only for printing classified information, then passed those sheets to CJ. So, the problem is a lax attitude toward the protection of classified information on the parts of both persons and anyone else who saw sheets of colored paper outside the SCIF. And kudos to the anonymous tipster.

Accepted Practice.

Everyone does it, right? In this sort of situation, we assume that everyone is responsible for security in their space. But, in fact, no one is in charge. Chelsea Manning captured 250,000 classified cables and intelligence reports by loading them onto CD-RW's labelled "Lady Gaga" while she was working inside a SCIF in Iraq. The question is, what to do about this? Possible response: have the IT team load scads of music onto the classified servers so people can listen legally.

Concerned Co-Worker.

Matt's grandmother died. He's been dealing with his own grief, arrangements for the funeral, and managing her estate, while still getting his work done at HRG-KB. She left him the car in her will. Matt plans to use part of his inheritance to buy himself a used 24’ center console boat—hardly a yacht. Karyn would probably admit that she just doesn’t like Matt.

The Problem with Partners 1.

Is this a question of dual-use technology, a breach of security, or something else? It’s hard to say with only the information you’ve been given but this needs to be addressed. If the technology the partner researcher is developing in her unclassified program at MTI is substantially the same as that she’s developing under the HRG-KB grant, there might be a problem. She can believe what she wants to believe about the importance of sharing information vs. security, but she will have signed a non-disclosure agreement when she was granted a security clearance, and if she has released classified information (either wittingly or unwittingly) she may be in breach of that agreement.

The Problem with Partners 2.

This might be a problem. It’s hard to say given the information you have at hand. It is possible that the facets of the technological research Dr. Preieto has farmed out to her new foreign office aren’t related to the research she’s doing with HRG. The U.S. intelligence community regularly shares intelligence with foreign nations—NATO and the Five Eyes alliance (U.S., UK, Canada, Australia, and New Zealand) readily come to mind. Material to be shared with partner organizations must be cleared by the responsible foreign disclosure office. It’s probably worth reporting this to the Defense Department security team just in case.

Culture Clash.

The employee came to HRG from Caltech where she held a prestigious, named research chair. Getting her was considered a major coup for the research director. She is a tremendously talented scientist who seemingly has little time for what she considers pointless protocols. She came from an academic culture where moving data from one computer system to another was a simple process—load it on a flash drive and move it. She is unaccustomed even to having different computer systems (NIPR, SIPR, JWICS, etc.) on her desk. The security manual that explains HRG’s security policies and procedures sits on a shelf in her office in its original packaging, unopened. When asked where she got the flash drive, she says she bought it at a small shop just outside the Navy base over the weekend.

Clicks.

What CJ believes and how he expresses himself is his business—to a point. But if his behavior is erratic enough to raise concerns among his co-workers and managers, the organization needs to figure out what its options are.

Save the Whales.

Kristi Penn's daughter, Kara, is wittingly passing information on the boat schedule that she gleans from Kris in everyday family conversation to a friend who is a member of PAAR.

Glossary

C-Suite. The suite of office spaces where an organization's most senior officers work. The "C" stands for chief as in chief executive officer, chief operating officer, chief information officer, and so on.

Class 5 Container. A General Services Administration-approved steel safe with a combination lock.

JWICS (Joint Worldwide Intelligence Communications System). A data communications network used by U.S. military and civilian intelligence agencies to transmit, receive, and store top secret, code word, and sensitive compartmentalized information.

NIPRNet (Non-classified Internet Protocol Router Network). The U.S. military's unclassified computer network.

PROPIN (Proprietary Information). A special handling caveat used on certain classified information "provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value."

Secret. A classification level between confidential and top secret. Information classified secret "reasonably could be expected to cause serious damage to the national security."

SCIF (Sensitive Compartmented Information Facility). Within a building or compound, an area set-aside for processing sensitive compartmented information (see below).

Sensitive Compartmented Information (SCI). SCI is a subset of classified national intelligence that takes into account the source and method of acquisition of the information. It is not a higher level intelligence than collateral Top Secret, the designation simply means that it requires special handling because of the source(s). It may only be stored and viewed inside a sensitive compartmented information facility (SCIF).

SIPRNet (Secret Internet Protocol Router Network). The U.S. military's secret-level classified network.

Top Secret (TS). A classification level above secret. Information classified as top secret "reasonably could be expected to cause exceptionally grave damage to the national security."

Additional Scenario Development

Later in the period of performance, further funds were allocated to this seedling for the development of two additional scenario designs. Simulation designers at The ICONS Project created two additional scenarios based around supply chain management and security. The two scenarios examine both outbound and inbound supply issues.

1. Outbound. An item shipped from HRG-KB to a partner organization has disappeared. It was packed by loading dock staff under the supervision of both the R&D team who developed the piece of technology, and the transportation team supervisors. The package was picked up for delivery by a trusted local transportation company the next morning but did not arrive at the Maritime Technology Institute on schedule. Two HRG-KB Staff members have unrestricted access to the area where the package was stored overnight. Both were, at different times, in the area alone. What happened? (This will likely be an external threat involving the driver for the local transportation company.)

2. Inbound. A routine scan of computers revealed malware installed and active on a desktop computer in the HR section's offices. The machine, newly installed, was connected to the HRG-KB local network and had access to the world-wide web via ethernet. It was in place for 24 hours before the discovery. It has been removed, isolated, and is being examined by the IT and security teams. What happened? (This will likely be a question of following or not the best practices used industry and government-wide for procurement of computers.)

As this additional funding was not available until September 2021, the team includes this brief summary description for the final deliverable report. The full scenario descriptions (similar to the one provided in the main body of this report for the initially funded work) will be available upon request as part of the ICONSnet catalog.

ACKNOWLEDGEMENTS

This report was prepared for [Office of the Undersecretary of Defense for Intelligence and Security (OUSD(I&S)), United States Department of Defense (DoD)] under the following agreement: HQ003420F0655, *University of Maryland,* "Insider Threat and Personnel Vetting."

DISCLAIMERS

Any views, opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of an official United States government position, policy, or decision. Additionally, neither the United States government nor any of its employees make any warranty, expressed or implied, nor assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in this publication.

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the Applied Research Laboratory for Intelligence and Security (ARLIS), the University of Maryland, or the United States government, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

ABOUT ARLIS

Applied Research Laboratory for Intelligence and Security (ARLIS) is a UARC based at the University of Maryland College Park and established in 2018 under the auspices of the OUSD(I&S). ARLIS is intended as a long-term strategic asset for research and development in artificial intelligence, information engineering, acquisition security, and social systems. One of only 14 designated United States Department of Defense (DoD) UARCs in the nation, ARLIS conducts both classified and unclassified research spanning from basic to applied system development and works to serve the U.S. Government as an independent and objective trusted agent.

ABOUT START

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a university-based research, education and training center comprised of an international network of scholars committed to the scientific study of terrorism, responses to terrorism and related phenomena. Led by the University of Maryland, START is a Department of Homeland Security Emeritus Center of Excellence that is supported by multiple federal agencies and departments. START uses state-of-the-art theories, methods, and data from the social and behavioral sciences to improve understanding of the origins, dynamics, and effects of terrorism; the effectiveness and impacts of counterterrorism and CVE; and other matters of global and national security. For more information, visit www.start.umd.edu or contact START at infostart@umd.edu.

Technical Points of Contact

PI: Adam Russell, D.Phil.
Chief Scientist, ARLIS
301.226.8834; arussell@arlis.umd.edu

Co-PI: Kelly Jones, Ph.D.
Assistant Research Scientist, ARLIS
301.226.8850; kjones@arlis.umd.edu

Task Lead: Devin Ellis
Director of the ICONS Project
Senior Faculty Research Specialist, ARLIS
203.586.9697; ellisd@umd.edu

Administrative Points of Contact

Ms. Monique Anderson
Contract Officer, Office of Research Administration
Assistant Director, ARLIS
301.405.6272; manders1@umd.edu