# The Three M's of the Cybersecurity Insider Threat Revealed

By John Galliano, Contributing Editor

What do you think of when you hear the term cybersecurity? You might associate the term with computer security, or information security, or information assurance. You may think of vulnerability management and malware, viruses, or malicious hackers attempting to breach your network defenses from the outside. Very likely, as a military cyber professional, you work in well secured environment with next-generation firewalls, intrusion detection/prevention and other specialized sensors to safeguard your perimeter and protect your organization's information. But how often do you consider your internal defenses and the trusted people already on the inside?


The cyber insider threat is not a new problem. Operating from the inside and unconcerned with perimeter defenses, U.S. Army Private Bradley Manning had access to the Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNet). In 2009, Manning used that trusted access to pass an estimated 250,000 sensitive State Department diplomatic cables[1,2] containing privileged communications with over 300 consulates, embassies, and diplomatic missions to Wikileaks.

More than one third of the documents were classified confidential or secret[3]. This unauthorized leak embarrassed the DoD and US Government and likely damaged relationships with friendly countries. The remediation in terms of enhanced controls while needed, has no doubt been costly.

Manning's actions underscored that insiders represent the greatest security risk impacting organizations[4] and may represent the weakest link in your overall security posture[5]. In fact, the research firm Cybersecurity Insiders in partnership with Crowd Research, surveyed 472 cybersecurity professionals and the majority of respondents confirmed insider attacks had occurred against their organization in the previous 12 months[6], while twenty-seven percent stated insider attacks had become more frequent. In addition, ninety percent of organizations surveyed felt vulnerable to insider attacks[7,8]. According to the 2017 Verizon Data Breach Investigations Report (DBIR), one of every four data breaches are attributable to cyber insiders[9].

There are financial impacts to consider as well. The Ponemon Institute's recent study of 159 global organizations pegged the average cost of an insider threat at $8.7 million[10] and in 49 cases studied by Carnegie Mellon researchers, losses reached the tens of millions[11]. Beyond cost, organizations spend an average of 74 days to recover from an insider threat attack[10] with three-quarters of respondents experiencing a significant impact to business operations[11]. Clearly, the insider threat is an important issue.

These statistics are sobering and should be of concern to military cyber professionals. Simply put, a failure to understand the cyber insider threat puts your organization, your data, and your people at heightened risk. In this article, we will take a look at the meaning, the motivation, and the mitigation of the cyber insider threat. Let's begin by first taking a look at the meaning of the insider threat.

## The Meaning

What is a cyber insider threat and how does the cyber insider threat differ from the more traditional understanding of insider within the realm of counter-intelligence?

Carnegie Mellon University's Software Engineering Institute defines a malicious insider as, "a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability [C-I-A] of the organization's information or information systems"[12]. From the cyber perspective then, the insider threat is basically any threat involving the information or the technology encompassing the network. We should be careful to note that while the cyber insider threat can be of malicious intent and result in potentially severe consequences, not every threat rises to the level of an Edward Snowden or Bradley Manning in scope nor damage. Sometimes, we are simply the victims of misconfiguration, unintended errors, or user negligence as examples of other potential root causes.

The term *insider* cuts right to the core of the matter. At the Defense Information Systems Agency (DISA), the cyber insider threat is seen as both prevalent and important enough that an entire section is dedicated to proactively monitor, quickly surface, and properly socialize suspicious behaviors within fusion areas of expertise exists. This approach has allowed the agency to facilitate an accurate threat assessment and recommend proactive mitigations to leadership. Paul Demennato, Chief of the Cybersecurity Insider Threat Division at the DISA, stated, "once someone receives permission to access what is denied to outsiders, the cyber kill chain is already in place. They're already a trusted person. They're already inside"[13]. Figure 1 depicts the cyber insider within the traditional cyber kill chain.

Coupled with other enabling risk factors, for example, excessive access privileges, the proliferation of mobile and other devices (including Internet of Things (IoT)) with access to sensitive data, and the expanding complexity of information technology, the result is an environment that is especially vulnerable to human factors. With a solid definition and context in mind, we can move to the motivating factors.

## The Motivation

Why do insiders, the people we have brought into the fold and trusted, choose to engage in malicious activities? While there are numerous reasons, we

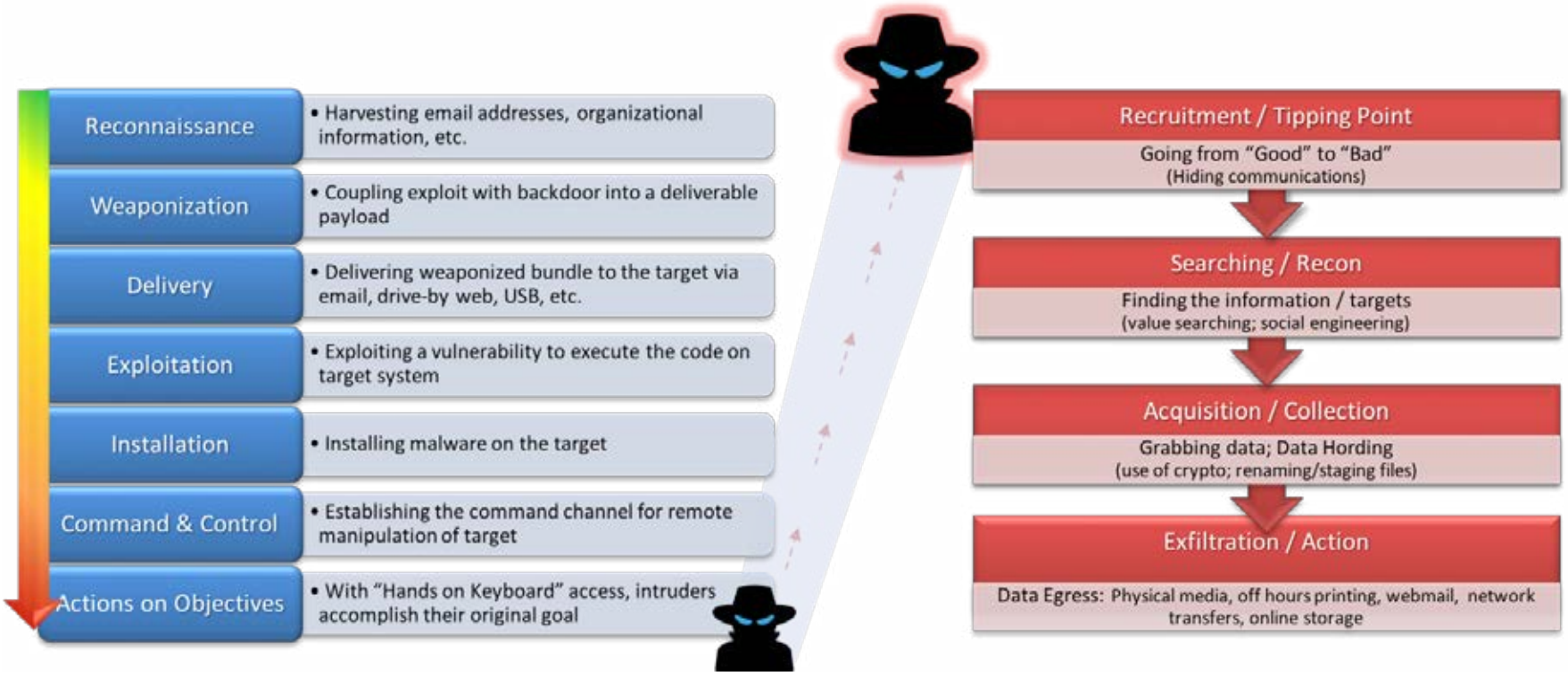


Figure 1. The Cyber Kill Chain in the Insider Threat Context, adapted from "Intelligence-Driven Computer Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain" by Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011) in Leading Issues in Information Warfare & Security Research, 1(1), 80.

will focus on the areas of personal gain, getting even/perceived injustice, and the greater cause.

*Personal gain*–The need or desire for money, stemming from hard times, poor financial management, greed, sudden purchases of high value items or living beyond financial means. This motivator can result in all manner of illicit activities including modifying or stealing confidential or sensitive information, theft of intellectual property, national security related information or secrets, or personnel information to sell to a foreign government or entity. An example of personal gain may be gleaned from the Anthem health insurance company breach of a few years ago, which contained a relevant insider threat element. An employee emailed sensitive personal health information (PHI) data about Anthem's customers including Medicare ID and Social Security numbers, names, and dates of enrollment to his personal email address. Do you allow webmail in your environment? If so, do you watch for suspicious activity that may indicate data exfiltration? Another example gleaned from the Carnegie Mellon Insider Threat Management and Education of the Risk of Insider Threat (MERIT) database[14] recounts the story of a group of insiders (collusion, anyone?) at a wireless telecommunications firm. These employees cloned 16,000+ customer mobile phones over a period of six months, illegally profiting from unauthorized calls valued at $15 million[15].

*Getting Even/Perceived Injustice* – These people feel wronged by the organization. They are the employee with the proverbial axe to grind with access to the organization's sensitive data (and may also possess privileged access). The Australian Department of Defense found that an astounding 70 percent of known malicious insiders had been previously reprimanded for inappropriate behavior! Be alert for indicators such as odd work patterns, arguing with coworkers, poor performance, and pronounced irritability/vocalization of wrongs[16]. In 2012, Hannah Robert, provided export-controlled, sensitive documents about U.S. military weapons programs to an Indian national. Robert exfiltrated the data to her church's website, where she volunteered as a web admin and used the electronic dead drop to compromise torpedo systems, F-15 fighter aircraft, and attack helicopters. Robert also conspired to supply faulty parts to the U.S. Air Force, an act that resulted in costs exceeding $150,000 in repair and re-inspection costs[17]. Thus, there is ample justification for the increased scrutiny of reprimanded employees.

*The Greater Cause* – Employees may be motivated by strong political or religious beliefs. They may take actions and practice risky behaviors as a result. In addition, an outside influence may be at play. The Forrester Research Group highlighted that malicious insiders may be blackmailed or coerced into taking actions by a crime ring or nation-state actor[18].

There is perhaps no greater example than Snowden's release of a trove of National Security Agency (NSA) and Government Communications Headquarters (GCHQ) documents, many of which were classified at the Top Secret level. Snowden saw himself as a patriot exposing the post-9/11, surveillance state and was widely celebrated for his actions by hacktivists and civil libertarians[19]. Perspective notwithstanding, Snowden clearly abused his insider access and knowledge to carry out his surreptitious collection of classified information and pass it to the press.

Disgruntled employees, the financially strapped, and those motivated by a cause have knowledge of and access to your sensitive and classified information. These people are already on the inside and may be able to legitimately bypass security measures. Or, they may know someone who can.

We have placed the cyber insider threat into a deeper context and gained a better appreciation for the motivating factors involved. What can we do as military cyber professionals to mitigate the cyber insider threat?

## The Mitigation

The research indicates that malicious insiders typically share common motivational factors that cause them to target your information assets, technology assets, or even financial assets. Mitigation consists of the tangible activities your organization can put into practice to counter the cyber insider threat. These are the elements that we utilize to dissuade and deter the insider from engaging in malicious acts. Our aim here is to raise the cost or to make the insider think twice prior to acting. In this article, we will focus on education, monitoring, and controlling.

Education, in the form of training and awareness, is arguably the foundation of a proactive approach

to detection and prevention. The National Institute of Standards and Technology (NIST) suggests that security assessors should, "determine if the organization includes security awareness training on recognizing and reporting potential indicators of insider threat"[20]. In addition, the National Insider Threat Task Force (NITTF) provides technical and program assistance, conducts training, and disseminates insider threat program best practices[21]. Leverage your organization's larger insider threat program, if available. Seek out your cyber insider threat and counter intelligence specialists and ask them how you can best support their efforts.


We must go beyond the obligatory annual awareness training. Experts widely agree that establishing a collective responsibility in protecting company information is a critical facet in an insider threat program[22]. Making use of regular messaging, awareness, and workforce communications will ensure a greater degree of preparedness to recognize and respond to insider threats. Education, then plays an important a role.

With monitoring, it's all about the logs, logs, logs. A study of cyber incidents in the telecommunications sector revealed that 57% of detections were made via anomalous indicators seen in access logs[8]. With such a high rate of success, it follows that your organization needs a log retention policy, the storage to ingest logs for use in a log reduction tool, and the active monitoring and analysis of logs to effectively recognize abnormal and suspicious behaviors.

A solid analysis and correlation of logs will individual usage and behavioral anomalies, which may facilitate more timely response actions and minimize potential damages in the event of an insider breach.

But log analysis alone is not sufficient. Monitoring other indicators of compromise (IoCs) can be achieved from implementing the countermeasures in NIST SP 800-53, Appendix G, which includes a mapping of additional controls to the insider threat[20]. These additional controls are shown in Table 1 on the opposite page.

Beyond these basic cyber hygiene monitoring tools, the next logical step includes implementing User Activity Monitoring (UAM) and User and Entity Behavior Analytics (UEBA) in the form of tools that can be employed to effectively detect malicious insiders engaging in anomalous or otherwise suspicious activity. UEBA, in particular, leverages the use of data mining and analytic visualization tools. Remember that these advanced tools can introduce (in some cases, significant) privacy concerns, therefore you should strategically communicate why the tools are employed, how the tools can improve security, and how the tools can be used to proactively safeguard organizational information[22]. Get your people on board.

The final focus of mitigation is control. A 2008 study revealed the single greatest cause of successful cyber insider threat attacks in the government sector was privilege escalation[8]. Further, CyberArk Software recommended that organizations "minimize user privileges to reduce the attack surface, lock down privileged credentials, and control and monitor privileged accounts, which are consistently targeted by [the] advanced insider…"[23]. Thus, controlling who in your organization has elevated privileges is absolutely critical. In addition, provisioning privileged access should be based on the principle of least privilege, based on specific duties and the separation of roles, and regularly audited to ensure access is curtailed when no longer required[24].

The cyber insider threat should be of concern to military cyber professionals because it puts your organization, your data, and your people at heightened risk. In this article, we looked at the meaning, the motivation, and the mitigation of the cyber insider threat. We learned that insiders in the context of cybersecurity have access to an organization's network, system, or data and intentionally exceeded or used that access in a manner that negatively affected the C-I-A of the organization's information or information systems.

Insider threat attacks are costly both in terms of time and money, and ultimately may put military operations and lives in jeopardy. Insiders are influenced by a range of motivations including personal gain, perceived injustice, and the greater cause. Finally, we examined a number of mitigating factors that may be employed to counter the potential impacts of the cyber insider threat including education, monitoring, and control. Implementing a strong and vigilant insider threat program is your first line of defense and your best protection.

**INSIDER THREAT MITIGATING FACTORS**

**EDUCATION**

**MONITORING**

**CONTROL**

*Table 1 – NIST 800-53 Insider Threat Related Controls.*

| | |
|---|---|
| **PM-12 (0) INSIDER THREAT PROGRAM** is the master control requiring an insider threat program, including a team focused on insider threat incident handling. The team needs to have cross discipline representation to monitor and correlate behavior patterns from different parts of the organization and in different forms. | **IR-4 (6) INCIDENT HANDLING \| INSIDER THREATS – SPECIFIC CAPABILITIES** –are added to the baseline during the control tailoring process to provide an emphasis on specific aspects of insider threat, how the organization intends to defend against the threat, and how to respond to the threat once detected. |
| **PM-1 INFORMATION SECURITY PROGRAM PLAN** lays out the foundation and framework for the entire security program. Incorporates requirements, roles, and responsibilities, and cross organizational coordination for dealing with insider threats. | **IR-4 (7) INCIDENT HANDLING \| INSIDER THREATS – INTRA ORGANIZATION COORDINATION** is the intra organizational cooperation needed to handle insider threats. |
| **PM-14 TESTING, TRAINING, AND MONITORING** is the security testing, training, and continuous monitoring of the insider threat. | **MP-7 MEDIA USE** is the restriction and/or prohibition of the use of specified types of media that can protect against unauthorized access, exfiltration of data, and unnecessary exposure to malware and other malicious logic. |
| **AC-6 (9) LEAST PRIVILEGE \| AUDITING USE OF PRIVILEGED FUNCTIONS** is an important control that prohibits privileged access to the information system by non-organizational users. | **PE-2 PHYSICAL ACCESS AUTHORIZATIONS** are the security protections that can limit the access that insiders already possess. It is important to carefully monitor and control physical access according to the level of protection required and the need of the individual to access a given physical area. |
| **AT-2 (2) SECURITY AWARENESS \| INSIDER THREAT** is the training needed to recognize indicators and the precursors of insider threat activities. | **PS-3 PERSONNEL SCREENING** takes into account the processes that include the variable conditions/frequencies based on the types of information to be protected. |
| **AU-6 (9) AUDIT REVIEW, ANALYSIS, AND REPORTING \| CORRELATION WITH INPUT FROM NON-TECHNICAL SOURCES** is the correlation of non-technical input with audit data that can reveal patterns of potential insider threat activities. | **PS-4 PERSONNEL TERMINATION** such as good exit interviews and promptly disabling system access and revoking credentials can prevent problems that arise from disgruntled employees under termination. |
| **AU-7 AUDIT REDUCTION AND REPORT GENERATION** is the audit data that can be filtered to reduce data size while facilitating concentration on specific issues, for example unauthorized insider activities. | **PS-5 PERSONNEL TRANSFER** are access control status changes resulting from individuals who are reassigned or transferred. |
| **AU-10 NON-REPUDIATION** is the mechanism that denies the malicious insider from carrying out their activities. | **PS-8 PERSONNEL SANCTIONS** are the policies and procedures that must be enforced with penalties in order to be effective. |
| **AU-12 AUDIT GENERATION** are the definable parameters that focus the audit trail on insider activity of concern and deter the insider's ability to make changes. | **SC-5 (1) DENIAL OF SERVICE PROTECTION \| RESTRICT INTERNAL USERS** are the policies that restrict or limit the ability of insiders to use components of the information system to launch denial of service attacks. |
| **AU-13 MONITORING FOR INFORMATION DISCLOSURE** is the definition and monitoring of designated sites for evidence of information disclosure. | **SC-7 BOUNDARY PROTECTION** is managing interfaces at both external and internal boundaries to reduce unauthorized access and information flow. |
| **CA-2 (2) SECURITY ASSESSMENTS \| TYPES OF ASSESSMENTS** are the selectable parameters that offer a variety of security assessments, including a focus on the insider threat. | **SC-7 (9) BOUNDARY PROTECTION \| RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC** detects outgoing traffic that can pose a threat to other systems and identify the associated internal users. |
| **CA-7 CONTINUOUS MONITORING** is designed to raise awareness of the current functioning status of controls, the security posture of the system, and any change in the status of threats or vulnerabilities in relation to the security posture. As such, these metrics can be focused on controls that provide protection against insider threats. | **SC-7 (10) BOUNDARY PROTECTION \| PREVENT UNAUTHORIZED EXFILTRATION** manages the interfaces to detect and prevent against unauthorized data movement or exfiltration. |
| **CP-2 (1) CONTINGENCY PLAN \| COORDINATE WITH RELATED PLANS** is the need for an insider threat plan that can be integrated into the contingency plan (CP) and coordinated with other parts of the CP. | **SC-38 OPERATIONS SECURITY** are the tactics, techniques, and procedures used to identify information of interest to insider threat actors. |
| **IA-4 IDENTIFIER MANAGEMENT** is a good certification process that protects against allowing inappropriate insider access; identifying user status and coordinating the management of identifiers to protect against the sharing of information with insiders inappropriately. | **SI-4 (12) INFORMATION SYSTEM MONITORING \| AUTOMATED ALERTS** are the mechanism used to focus attention on anomalous activities and appropriately surface that information in a timely and relevant manner. |

*Dr. Galliano is a multi-certified computer security expert. His passion is writing and sharing insights gained in the cybersecurity field. His interests include ethical hacking, certification development, digital forensics, and applying research-based cybersecurity solutions to the enterprise. His expertise lies in insider threat, incident response and forensics, and network security. Dr. Galliano obtained his Doctorate in Information Assurance from the University of Fairfax with a specialization in cybersecurity. He teaches undergraduate cybersecurity courses at the University of Maryland and participates in the UMUC cyber competition team, the Cyber Padawans.*

1.K. Poulsen, "WikiLeaks and the Massive Data Dump That Rocked the Pentagon," Wired Magazine, 2013. [Online]. Available: https://www.wired.com/2013/04/wikileaks/. [Accessed: 08-May-2018].. [Accessed 08 05 2018].
2.T. Sorell, "Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous," Journal of Human Rights Practice, vol. 7, no. 3, pp. 391-410. https://doi.org/10.1093/jhuman/huv012, November 2015.
3.H. Berghel, "WikiLeaks and the Matter of Private Manning," Computer, IEEE Computer Society, Vols. 0018-9162, no. 12, pp. 86-89, 2015.
4.S. Payne, "Developing Security Education and Awareness Programs," Education Quarterly, vol. 26, no. 4, pp. 49-53, 2003.
5.T. Tryfonas and T. Fagade, "Malicious Insider Threat Detection: A Conceptual Model," Security and Protection of Information, no. June, pp. 31-44, 2017.
6.P. Fersht, R. LaSalle, F. McClimans, R. Phelps and J. Snowdon, "The State of Cybersecurity and Digital Trust: Identifying Cybersecurity Gaps to Rethink State of the Art," Accenture and HFS Research, Ltd., Washington, DC, 2016.
7.H. Schulze, "Insider Threat 2018 Report," Cybersecurity Insiders in partnership with Crowd Research, Baltimore, MD., 2018.
8.D. Cappelli, E. Kowalski and A. P. Moore, Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector, Pitssburgh, PA: Carnegie Mellon University Software Engineering Institute, 2008.
9.Verizon Enterprise, "2017 Data Breach Investigation Report, 10th Ed., p.3," Verizon, Inc., New York, NY, 2017.
10.Ponemon Institute LLC, "2018 Cost of Insider Threats: Global Organizations," ObserveIT, Traverse City, MI, 2018.
11.D. M. Cappelli, A. G. Desai, A. P. Moore, T. J. Shimeall, E. A. Weaver and B. Willke, "Management and Education of the Risk of Insider Threat (MERIT): mitigating the risk of sabotage to employers' information, systems, or networks," Defense Technical Information Center (DTIC). Availalbe at http://www.dtic.mil/dtic/tr/fulltext/u2/a468801.pdf., Pittsburgh, PA., 2007.
12.D. Cappelli, R. Moore, R. F. and G. Silowash, "Common Sense Guide to Mitigating Insider Threats," Software Engineering Institute, Pittsburgh, PA, 2012.
13.Digital Reasoning, Composer, Executive Briefing Series: Insider Threat. [Sound Recording]. Federal News Radio. 2017.
14.R. Trzeciak, "Insider Threat Blog, The CERT Insider Threat Database," Carnegie Mellon University Software Engineering Institute, 2011. [Online]. Available: http://www.cert.org/blogs/insider_threat/2011/08/the_cert_insider_threat_ database.html. [Accessed 6 May 2018].
15.ObserveIT, "5 Examples of Insider Threat-Caused Breaches," 22 March 2018. [Online]. Available: https://www.observeit.com/blog/5-examples-of-insider-threat-caused-breaches/. [Accessed 6 May 2018].
16.M. Butavic, A. McCormac and K. Parsons, "Preventing and Profiling Malicious Insider Attacks. Technical Report #DSTO-TR-2697," Australian Government Department of Defence, Edinburgh, South Australia, 2012.
17.Center for Development of Security Excellence (CDSE), "Hannah Robert Case Study," 2016. [Online]. Available: https://www.cdse.edu/documents/toolkits-insider/hannah-robert-case-study.pdf. [Accessed 9 May 2018].
18.J. Blankenship, "Hunting Insider Threats," Forrester Research, Cambridge, MA, 2016.
19.D. Fisher, C. Halladay and F. Moghaddam, "The Millennial Generation as an Insider Threat: High Risk or Overhyped?," Naval Postgraduate School (NPS), Monterey, CA, 2015.
20.R. Ross, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans (No. Special Publication (NIST SP)-800-53A Rev 4).," National Institute of Standards (NIST), Washington, DC, 2014.
21.National Insider Threat Task Force (NITTF, "Guide to Accompany the National Insider Threat Policy and Minimum Standards," NITTF, Washington, DC, 2013.
22.RSA Cybersecurity Conference, "2018 Global Insider Threat Summit," in Expert Panel, San Francisco, CA. https://www.rsaconference.com/events/us18, 2018.
23.CyberArk, "The Danger Within: Unmasking Insider Threats. www.cyberark.com/solutions/security-risk-management/insider-threats/," CyberArk Software, Inc., Newton, MA, 2016.
24.D. M. Upton and S. Creese, "The danger from within," Harvard Business Review, vol. 92, no. 9, pp. 94-101, 2014.

Image credits (in order of appearance): Original Artwork, [See Caption], Unknown (Facebook Post Meme)