DoD Has Over 3.5 Million Insiders – Now What?

A User Online Risk Score Framework To Reduce The Insider Threat

Lieutenant Colonel (P) Stephen A. Roberts, Ph.D.

ABSTRACT

DoD employs about 3.5 million military and civilian direct employees, contractors, and reserve personnel. In addition, over 50,000 contracted entities (e.g., groups and organizations) can connect directly to the DoD Information Network (DoDIN) to collaborate and protect DoD systems and sensitive data. These imperfect users often interact with DoD across multiple classification domains and IT systems. Without focusing on potentially damaging insider activity, DoD will fail to meet the 2018 Cyber Strategy objectives, and adversaries will continue to erode our technical overmatch while imposing excessive remediation costs. This erosion occurs not only through attacks using technical means but also through exploitation of insiders. This article will introduce and urge the implementation of a framework to more effectively address insider threats by providing an empirical measure of each user's risk through their actual behaviors. This model will give the user near-real-time awareness of personal behaviors counter to organizational policy and cybersecurity requirements. This measure will also empower management to target training, remediation, and risk reduction while also allowing decision-makers to determine which user risk-exposed areas, roles, or practices require additional remediation. As a result, all organizational decision levels will be better able to improve cybersecurity resiliency in the face of an ever-evolving insider threat landscape.

INTRODUCTION

To fully achieve the latest Cyber Strategy (2018) goals, DoD must effectively implement a comprehensive insider threat program. The National Insider Threat Policy and Minimal Standards for Executive Branch Insider Threat Programs (EO 13587) and DODD 5205.16 outline requirements for an insider threat program (2012

Lieutenant Colonel (P) Stephen A. Roberts, Ph.D., a 30-year DoD veteran, is a Cyber Branch Officer now serving as the ARCYBER G30 LNO at Fort Meade, MD, and previously served a yearlong Senior Service College Cyber fellowship at Carnegie Mellon University. He holds a Bachelor of Science in Computer Information Systems, three Masters of Science (Computer Science, Computer Forensics, and Government Information Leadership with emphasis on Cybersecurity), and a Ph.D. in Cybersecurity with an emphasis on Insider Threat. He holds certifications as a Federal Chief Information Officer (CIO), Federal Chief Information Security Officer (CISO), CNSS/NSTISSI 4011, 4012, 4015, 4016, Security Plus, and CISSP.

and 2014 respectively),[1] which cover user awareness training along with monitoring and detection of malicious insiders, but make no mention of non-malicious insider activity. Today, years after these standards were first codified, a 2018 DoD Inspector General (IG) report confirms non-compliance with these minimal policy standards.[2]

Without focusing on potentially damaging insider activity, DoD will fail to meet the 2018 Cyber Strategy objectives.[3] More importantly, adversaries will continue to erode our technical overmatch and impose excessive remediation costs. This erosion occurs through attacks using technical means as well as by exploiting malicious and non-malicious insiders.[4] This article urges the immediate implementation of an empirical user behavior measurement framework to drive individual awareness, compliance, and accountability, which will reduce an adversary's ability to conduct daily operations and enable management to more effectively address the insider threat. It will also allow senior leaders to see organizational cybersecurity strengths and weaknesses at the user level, allowing the empirical decision support that is lacking today.

Malicious Insiders

Malicious insiders are organizational users with access and hence have a unique ability to exploit information technology (IT) assets to harm the organization, its customers, or its employees.[5] While representing a tiny percentage of the workforce, these insiders often plan and execute attacks over long periods of employment,[6] and their impact can psychologically devastate entire organizations. In addition, these trusted actors interact personally with colleagues as team members and, with no warning, betray organizations with a level of deceit that devastates colleagues and organizational cultures for long periods.[7] The US has suffered its share of significant malicious insider incidents, such as Private Manning, Edward Snowden, and Robert Hanssen.[8]

The impact of each successive compromise increases as the data accessible within IT systems also expands. These losses have led to reactionary and wholly inadequate policy changes to prevent compromise recurrence.[9] The apparent daily loss of personal information and intellectual property compounds injury caused by these malicious insider events. Collectively, insider-attributed losses continually add to what has been identified as the most significant transfer of wealth and knowledge in human existence.[10] Moreover, these compromises are not only attributable to the malicious insider but also the non-malicious insider.

Non-Malicious Insiders

DoD must continue to pursue programs to identify and manage the unique malicious insider threat. Still, non-malicious insiders can also have devastating, long term impacts, given their ongoing, sometimes multi-year interaction and decision-making related to DoD IT systems.[11] Non-malicious insiders typically make a myriad of poor decisions (e.g., by clicking on spam email links, misplacing Common Access Cards [CAC], leaving devices unlocked, visiting insecure websites, introducing malware onto networks, leaving government assets unsecured, or ferrying DoD data across home and public resources). These imprudent actions are often due to ignorance, impatience, gullibility, or the promise of a short-term increase in productivity.[12] The DoD employs about 3.5 million military and civilian direct employees, contractors, and reserve personnel.[13] In addition, over 50,000 contracted entities (e.g., groups and organizations) can connect to the DoD Information Network (DoDIN) to collaborate and protect DoD systems and sensitive data.[14] These imperfect human users often interact with the DoD across multiple classification domains and IT systems.[15] To illustrate the problem, if only 0.1% of the insiders produce one activity per year resulting in an incident, this equates to more than 3,500 annual incidents even if the impact of the contracted entity workforce is ignored.

Many of the same insider threats that plague the DoD also plague large commercial entities. For example, 85% of commercial sector data breaches involve human error. More troubling, the average time to detect a violation exceeds 220 days, and the time to correct an incident is an additional 80 days.[16] Meanwhile, the DoD also faces multiple, dedicated, nation-state-sponsored adversaries and advanced persistent threats (APT).[17] The adversarial threats patiently find and exploit the weakest link, which far too often is the insider.

A complete cybersecurity strategy includes technical, procedural, and physical controls.[18] DoD has implemented a complex cybersecurity model that implements a significant IT and technical security controls investment to combat global risks. The 2018 Cyber Strategy mentions many of these technical controls. Still, it seriously neglects the insider threat and the tools and awareness that senior leaders and managers need in order to identify or mitigate these issues. Generalized annual user awareness training is often the only tool leadership is provided with, which only marginally addresses the risk. In addition, security best practices prescribe an architecture with several layers of complementary defensive capabilities, commonly referred to as a Defense-in-Depth.[19] For example, a primary component of DoD's technology investment is the Joint Information Environment (JIE), representing $1 billion of its overall $42 billion annual IT investment.[20] Yet, despite this significant technological investment, either malicious or non-malicious insider actions can quickly defeat the effectiveness of these expensive technical controls.[21]

The DoD workforce provides the muscle, ingenuity, and productivity critical to mission accomplishment. It is also made up of imperfect humans. Research overwhelmingly confirms that humans are poor decision-makers regarding cyber risk evaluation and cybersecurity policy compliance.[22] Mere chance often prevents poor risk decisions from resulting in catastrophic compromise. Absent constant monitoring and behavior re-emphasis, poor behavior will remain a given. Lack of immediate adverse consequences leads to a new normal of self-serving or complacent behaviors until a costly cyber incident occurs at the hands of an opportunistic and patient adversary. Management and users typically do not acknowledge a problem until the breach is discovered, and the forensics, if conducted, uncovers the causative user activity. Often, these results may not be available for months or even years after the attack event.

Considerable research has sought to determine the reasons, behaviors, or triggers that cause woeful compliance by well-meaning users.[23] However, from a risk perspective, more important than the why of human behavior, is the existence and scale of this risk. Insider threat controls must manage this risk more completely. These controls must enable empirical management visibility, drive personal awareness and accountability, and target training that improves compliance and overall cybersecurity risk.[24] The DoD cannot leave cybersecurity at the user level to chance, given the stakes posed by near-peer adversaries with collectively greater resources, patience in achieving effects, and aggressive cyber exploitation policies.[25]

Recommended Strategy

Information Assurance (IA) training has been used to improve user cyber risk perception and decision making. The DoD has implemented mandatory annual training, but achieving 100% compliance has proven difficult, thus limiting the collective benefit. Research indicates that static training approaches, similar to those implemented by DoD, are ineffective.[26] Fear, punishment, and peer pressure mitigation approaches are equally weak.[27] Instead, mixing targeted training to raise specific user awareness and increased personal responsibility has proven more effective.[28] DoD should adopt these more dynamic approaches to optimize training efficiency better. Following an initial focus on base cybersecurity policies, individually measured risk behaviors that cover user gaps would overall raise the workforce's cyber efficacy and improve DoD's overall cybersecurity posture.

Using the Fair Isaac Corporation (FICO) credit score and creditworthiness model may be instructive for the next component of the recommended strategy. Used by the industry as an indicator of creditworthiness, a FICO score measures a person's credit trustworthiness based on historical financial behaviors and demographics.[29] Users can actively monitor their credit scores in many ways,[30] and this awareness significantly improves credit behaviors, knowledge, and average FICO scores.[31] FICO scores assist credit providers in making monetary trust decisions that will impact the provider and financial community of lenders and consumers alike. Monitoring applications allow users to see real-time changes in scores and provide training and guidance on improving scores.[32] Despite a lack of formal financial training, FICO monitoring educates and perceptibly alters behaviors that benefit the community and the user.[33] For the DoD, user cybersecurity monitoring would similarly provide a user-specific score by calculating compliance using various key measurement factors (e.g., Internet search patterns, email patterns, cyber policy adherence). This "online risk score" feedback can appear on the user's desktop screen to enable direct feedback and tailored training and instruction for specific behavioral challenges. Focused education would reduce non-compliance and stimulate positive score results, thus emphasizing healthier organizational cybersecurity behaviors.

This online risk score over time would be affected by a user's specific behaviors. Scores would be aggregated at several decision-making levels: individual, supervisory, departmental, and organizational, making users accountable for compliance behaviors and improving remediation visibility throughout the decision chain. Measuring personal and corporate accountability allows targeted management, mitigation, investment, and training at crucial risk sites and enables positive incentives and recognition for compliant behaviors. Scoring should be tailored over time to meet the changing threat landscape. Factors to track behaviors and their periodicity can reflect compliance trends (e.g., malware infections, data access patterns, and encrypted traffic patterns). Monitoring these scores would drive individual behavior change and provide the visibility required to address the aggregate insider threat effectively.

User Behaviors of Concern

Hiring employees costs time and money and lowers productivity while positions are unfilled and new employees learn their roles. Per-employee onboarding investments often exceed $4,000 and require up to eight months to gain full employee productivity,[34] which pressures employers to bring new employees to a productive state as soon as possible. Employers need to provide new employees with all the assets, data, and IT access necessary for them to do their job, employee productivity is a high priority. Several leading management books and best practices note that trust between management and the workforce is essential to achieve maximum productivity.[35] Whether personal or work-related, trust is critical to effective human relationships, but unearned or unwarranted trust can never be blindly assumed. Granting complete trust is more problematic in the information assurance (IA) and cybersecurity domains, where new employees very early on gain full access to critical organizational data and assets. On average, 17% of new hires depart in the first six months, and 26% leave within 12 months. Unearned trust and undue early access expose an organization to greater risk of data compromise, loss, or espionage.[36] Early trust often works out and thus promulgates the behavior. However, today the adverse impact in our highly connected world can be devastating (the average global cost per data breach is $3.6 million, the US average is over $8.6 million, with some violations exceeding $133 million. The OPM breach may approach $1 billion).[37]

Human evolution has allowed us to make sound life or death decisions in the physical world, but we are still groping for ways to recognize and counter virtual world threats.[38]

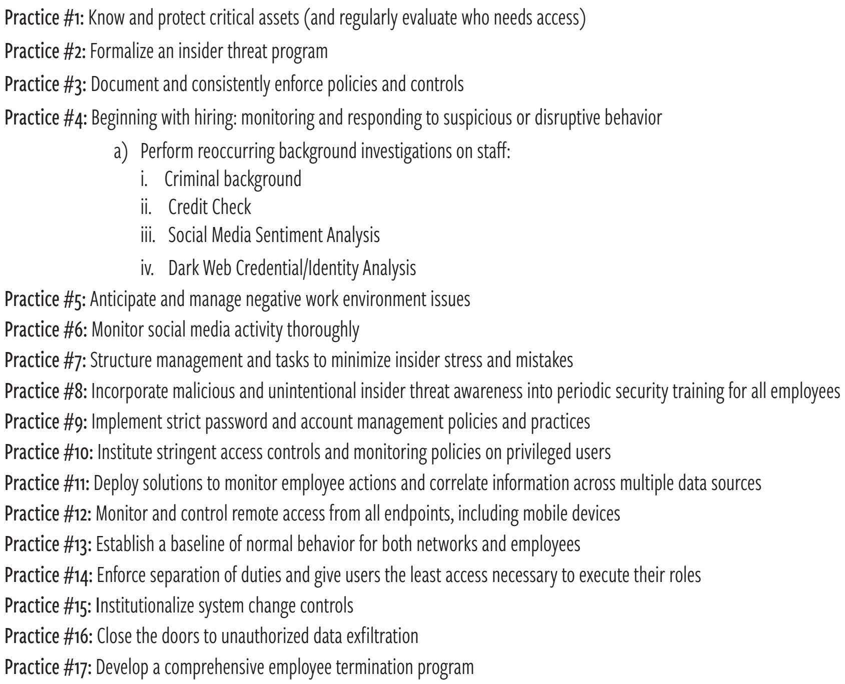
User behaviors that breach trust and compromise cybersecurity are an open research problem. A report co-sponsored by the National Institute of Standards and Technology (NIST) and the General Services Administration (GSA) found that only 26 of 789 journal articles and conference papers reviewed touched upon user behaviors. Most of these 26 lacked empirical data and specificity.[39] A review of 49 scholarly papers found similar results. Many discussed malicious insider behaviors and gave psychological explanations to help understand and detect such behavior, yet very few discussed non-malicious insider behaviors and actions that compromise security. Papers discussing non-malicious insiders focused more on user attitudes toward cybersecurity and information assurance policies without analyzing specific activities that compromise security. Understanding the psychology behind compromising user behavior is critically important, but these articles do little to help identify tangible mitigations, user accountability, or specific ways to change these troubling behaviors. A recent SANS Institute report identified causes for organizational endpoint compromise. The top reasons (representing 63% of all events) either directly or indirectly involved the internal user and the significance of the insider threat problem, and lists the following attack vectors involving the user:[40]

1. **Browser-based attacks:** visiting compromised websites that implant malware
2. **Social hacking:** clever spam messaging targeting groups or specific internal users
3. **Malicious external actors** interact with a trusting insider to gain sensitive organizational information (e.g., credentials, assets, data, or intellectual property)
4. **Ransomware:** typically delivered through organization-wide spam messages seeking at least one unwitting/malicious employee to enable the attack
5. **Credential theft or compromise:** theft or loss of an organization's asset, often stemming from carelessness in managing credentials, data, or equipment
6. **Infected, malicious USB or attached media devices** connect to the organizational IT infrastructure or connect remotely via an infected platform (e.g., home, hotel, Wi-Fi hotspot)
7. **Exploited common vulnerabilities and exposures (CVE):** disabling antivirus (AV) programs, blocking AV program updates, or preventing patch application for critical system software
8. **Compromised/unauthorized applications:** introducing compromised applications, enabling malicious software to run on corporate assets, or connecting to the organization's network via compromised off-network platforms

First published in 2008, the Verizon Research, Investigations, Solutions, Knowledge (RISK) Team Data Breach Investigations Report (DBIR) aggregated information security (IS) incident data analysis. The 2016 DBIR describes several problems directly enabled by internal user actions. Below are three of nine highlighted patterns that add context to the user risk score:

1. **Miscellaneous errors (17.7% of breaches):** 26% of these errors involved sensitive information sent to an unauthorized person, with the balance consisting mainly of internal human error or negligence.
2. **Insider and privileged account misuse (16.3% of breaches):** 34% of these were motivated by financial gain; 25% were linked to espionage.
3. **Physical theft and loss (15.1% of breaches):** 39% of these losses involved user workspace; 34% involved the user's vehicle.[41]

Based on a study of over 1,000 previous data breaches, the Software Engineering Institute (SEI) in 2016 updated best practices in reducing malicious insider risk, which is also relevant to developing a general risk score for all internal users. We will apply most of these practices to risk areas discussed in the prior reports:[42]



Practice #1: Know and protect critical assets (and regularly evaluate who needs access)

Practice #2: Formalize an insider threat program

Practice #3: Document and consistently enforce policies and controls

Practice #4: Beginning with hiring: monitoring and responding to suspicious or disruptive behavior

- a) Perform reoccurring background investigations on staff:
    - i. Criminal background
    - ii. Credit Check
    - iii. Social Media Sentiment Analysis
    - iv. Dark Web Credential/Identity Analysis

Practice #5: Anticipate and manage negative work environment issues

Practice #6: Monitor social media activity thoroughly

Practice #7: Structure management and tasks to minimize insider stress and mistakes

Practice #8: Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees

Practice #9: Implement strict password and account management policies and practices

Practice #10: Institute stringent access controls and monitoring policies on privileged users

Practice #11: Deploy solutions to monitor employee actions and correlate information across multiple data sources

Practice #12: Monitor and control remote access from all endpoints, including mobile devices

Practice #13: Establish a baseline of normal behavior for both networks and employees

Practice #14: Enforce separation of duties and give users the least access necessary to execute their roles

Practice #15: Institutionalize system change controls

Practice #16: Close the doors to unauthorized data exfiltration

Practice #17: Develop a comprehensive employee termination program

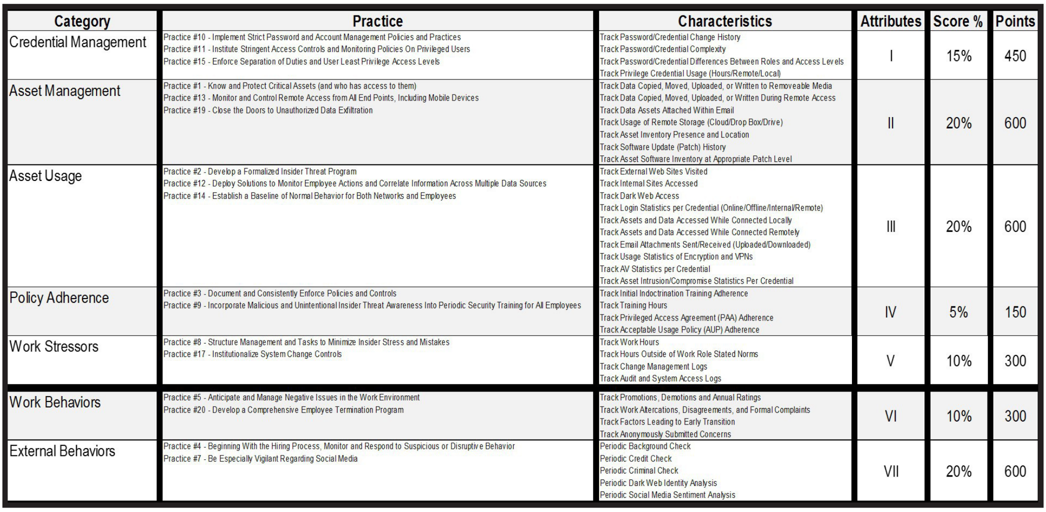
The DoD cannot afford to wait to implement a system that enables the awareness, responsibility, and methodology to improve cybersecurity and personal accountability. The solution highlighted here lacks production-grade testing and refinement. Still, it is prompted by conclusive proof of pervasive insider threats, both malicious and other, current cybersecurity practices, well-established research, and overwhelming forensic evidence. This recommended model is the first step in a process that would evolve to meet dynamic threats as production data helps to refine the framework.

Initially, the framework will use relative scoring and subjective weighting to tie user behaviors to compromise potential. The initial stages of implementation will drive user awareness and accountability, adding empirical certainty to the risk calculation. Weights, measures, and a scoring framework will help to gather feedback and refine the process, providing management with a more reliable picture of strengths and weaknesses, and optimize framework value and predictability over time.

Between 2008 and 2018, the Verizon DBIR has consistently characterized the insider threat impact and has made it clear that organizations will continue to suffer severe consequences if this threat isn't effectively addressed. The proposed User Online Risk Score (UORS) will provide a model for measuring and managing that portion of the cybersecurity threat.

Score Components

The UORS model relies on previous research and articles organized around seven differently weighted categories and uses a maximum of 3000 points, with points subtracted from each category based upon the initial draft framework represented in Figure 1 below.



Category	Practice	Characteristics	Attributes	Score %	Points
Credential Management	Practice #10 - Implement Strict Password and Account Management Policies and Practices Practice #11 - Institute Stringent Access Controls and Monitoring Policies On Privileged Users Practice #15 - Enforce Separation of Duties and User Least Privilege Access Levels	Track Password/Credential Change History Track Password/Credential Complexity Track Password/Credential Differences Between Roles and Access Levels Track Privilege Credential Usage (Hours/Remote/Local)	I	15%	450
Asset Management	Practice #1 - Know and Protect Critical Assets (and who has access to them) Practice #13 - Monitor and Control Remote Access from All End Points, Including Mobile Devices Practice #19 - Close the Doors to Unauthorized Data Exfiltration	Track Data Copied, Moved, Uploaded, or Written to Removeable Media Track Data Copied, Moved, Uploaded, or Written During Remote Access Track Data Assets Attached Within Email Track Usage of Remote Storage (Cloud/Drop Box/Drive) Track Asset Inventory Presence and Location Track Software Update (Patch) History Track Asset Software Inventory at Appropriate Patch Level	II	20%	600
Asset Usage	Practice #2 - Develop a Formalized Insider Threat Program Practice #12 - Deploy Solutions to Monitor Employee Actions and Correlate Information Across Multiple Data Sources Practice #14 - Establish a Baseline of Normal Behavior for Both Networks and Employees	Track External Web Sites Visited Track Internal Sites Accessed Track Dark Web Access Track Login Statistics per Credential (Online/Offline/Internal/Remote) Track Assets and Data Accessed While Connected Locally Track Assets and Data Accessed While Connected Remotely Track Email Attachments Sent/Received (Uploaded/Downloaded) Track Usage Statistics of Encryption and VPNs Track AV Statistics per Credential Track Asset Intrusion/Compromise Statistics Per Credential	III	20%	600
Policy Adherence	Practice #3 - Document and Consistently Enforce Policies and Controls Practice #9 - Incorporate Malicious and Unintentional Insider Threat Awareness Into Periodic Security Training for All Employees	Track Initial Indoctrination Training Adherence Track Training Hours Track Privileged Access Agreement (PAA) Adherence Track Acceptable Usage Policy (AUP) Adherence	IV	5%	150
Work Stressors	Practice #8 - Structure Management and Tasks to Minimize Insider Stress and Mistakes Practice #17 - Institutionalize System Change Controls	Track Work Hours Track Hours Outside of Work Role Stated Norms Track Change Management Logs Track Audit and System Access Logs	V	10%	300
Work Behaviors	Practice #5 - Anticipate and Manage Negative Issues in the Work Environment Practice #20 - Develop a Comprehensive Employee Termination Program	Track Promotions, Demotions and Annual Ratings Track Work Altercations, Disagreements, and Formal Complaints Track Factors Leading to Early Transition Track Anonymously Submitted Concerns	VI	10%	300
External Behaviors	Practice #4 - Beginning With the Hiring Process, Monitor and Respond to Suspicious or Disruptive Behavior Practice #7 - Be Especially Vigilant Regarding Social Media	Periodic Background Check Periodic Credit Check Periodic Criminal Check Periodic Dark Web Identity Analysis Periodic Social Media Sentiment Analysis	VII	20%	600

Figure 1. User Online Risk Score (UORS) Model

The UORS score would measure the relative risk each user represents compared to other users within the same work role and could be used to aggregate the relative risk that a work role, group, or division represents. In this way, leadership can use this tool to allocate limited resources to prioritized areas of manageable risk. In addition, over time, an organization may choose to modify the model to address future areas of risk that become a concern after initial implementation, analysis, and mitigation efforts.

The seven categories represent areas of significant risk posed by internal users.

1. **Credential Management.** Risk related to user choices accessing corporate assets with login credentials. Scores depict usage, change statistics, and credential separation between user access roles. Low scores may indicate poor user behavior or high-risk levels associated with work roles and access to critical assets. This area could indicate suboptimal organizational processes or the need for specific training or more segregated sensitive roles and accesses.
2. **Organizational Asset Management.** This category evaluates user behaviors in accessing organizational data and maintains assigned physical assets. This category also focuses on how the user accesses, copies, and modifies data. A low score may mean the user has placed organizational data or physical assets at a higher potential for compromise, which might require modification of asset management or inventory processes.
3. **Organizational Asset Usage.** This category focuses on user behavior insofar as exposing information technology (IT) infrastructure at risk by quantifying websites visited, emails sent and received, interactions with the antivirus program, and login specifics. Low scores could indicate the possibility of an asset or data breach by an external entity who was knowingly or unknowingly assisted by the internal user. This should trigger the information security (IS) response team to take immediate actions.
4. **Information Assurance (IA) Policy.** Adherence Scores rate user risk associated with policy knowledge, training, and IA/IS auditable practices, and the need for more or specific training.
5. **Work Environment Stressors.** This focuses on user work patterns that may drive higher stress levels and increase the chance of costly accidents, apathy, or destructive attitudes. Behaviors tracked include demand signals for work outside of regular business hours, work dissatisfaction, and involvement in operational environment changes. The confluence of additional off-duty work demands and corrections to production environments can increase risk and thus require employee work-life rebalancing or changes to production modification procedures.

6. **Work Environment Behaviors.** This category measures workplace events that could increase organizational risk exposure for employees or IT infrastructure. Events such as promotions, demotions, work-related altercations, formal complaint participants, compensation actions, staff ratings, and critical life changes are tracked to determine potential risks. Low scores may indicate a need for Human Resources Department or management intervention.
7. **External User Behaviors.** This category tracks non-workplace behavior that could increase risks to the organization, staff, and customer base. A 2009 report cited some 572,000 violent crimes committed at work or on duty,[43] many detectable with a pre-employment background check or by using periodic verifications/recertifications. This category would call for routine background checks, credit reports, social media sentiment checks, and Dark Web analysis. Employee stressors change throughout life and often can have devastating impacts on the organization.

Data Capture

Data required for an initial system build is mostly aggregated metadata, which comes from the existing data source systems. The UORS model would extract processed data from other solutions and data owners. Permissions from the data owners would be required. UORS would not require the raw data, only aggregated and processed statistics, thereby reducing UORS data storage requirements to less than the original system requirements. Data for the model would be drawn from the following sources.

1. Human Resources Department managed user-specific data (i.e., background check, promotion, evaluation, salary band information, formal and anonymous complaint statistics, regular work hours)
2. Password/Credential usage statistics from the authentication and authorization (AAA) solution
3 Virtual Private Network (VPN) statistics
4. Email statistics from mail servers and local computer clients.
5. User web usage statistics
6 Network architecture statistics associated with user equipment
7 Call detail records (CDRs) from organizational cellular billing solution
8. Office phone usage and CDR statistics
9 SharePoint and other knowledge management statistics
10. Antivirus (AV) statistics
11. Intrusion detection and firewall statistics.
12. Insider threat detection statistics
13. Inventory tracking system: specific equipment assigned to and in use by the user
14. Common Access Card (CAC) management statistics.
15. Windows profile, screensaver, and host policy statistics
16. High-profile employee usage statistics
17. Training department, acceptable use policy, and IT/IA training statistics.
18 Formal trouble ticket statistics associated with the user and their equipment
19. Physical security team: badge locations, hours, and in/out statistics.
20. Audit log and change management statistics.

Score Computation

The UORS sample framework is shown in Figure 1. Examples of detailed scoring charts are shown in Figures 2, 3, and 4 within Annex A. Although each category is broken into sub-components, some highlighted items are described below:

1. To counter the previously discussed tendency to initially trust new hires, the UORS model will lower the score (indicating higher risk) for unproven new hires, who have yet to assimilate with fellow staff, policies, practices, and workplace norms.

2. Employers who allow IT access before a complete background check or without executing periodic checks (credit, police, social media sentiment, Dark Web presence) will see the risk go up for affected employees.

3. US employees tend to work longer hours than those in other developed nations.[44] Moreover, immature organizations tend to push staff to work even harder and longer. Research strongly confirms that higher hours, late-night emails, answering work calls in off-hours, and being connected to the workplace at all hours are counterproductive and costly for both the employee and employer. Working long and dynamic hours significantly increases the risk of mistakes, employee fatigue, apathy, disgruntlement, unplanned time off, higher health care costs, turnover, espionage, or vandalism. Accordingly, the UORS model would reduce scores for long hours and dynamic off-hour work duties, especially for those with elevated privileges.[45]

4. The more a privileged account is used, the higher the risk for organizations. Best practices limit such use to necessary functions, separate roles, and accounts.[46] The UORS model would include high use in the risk score. Employee overuse of a privileged account, committing espionage, or an organization plagued with bad practices would all be scored low.

5. The more a user remotely accesses the IT infrastructure, selects links within an email, or accesses external websites, the lower the UORS score will be, in order to reflect this increased risk.

6. The UORS will account for Information Technology and Information Assurance policy and practice adherence. For example, inadequate awareness or training increases user risk.

Proposed Implementation

Implementation within the DoD would occur in phases, which would combine empirical rigor with DoD-specific data. The phased approach would also add functionality and value as the model matures. The first phase would include refining and adding probabilistic rigor to the model. The second phase would address platform security, user civil liberties, and privacy concerns that may affect complete deployment. During the first two phases, limited users would interact with the model output to allow testing, refinement, and model maturation.

The third phase would expand access while incorporating feedback to increase the tool utility, user awareness, and personal accountability desired. In addition, this third phase would include the organizational risk, training teams, and management to enable more effective targeted training and corporate risk reduction. The fourth phase would be a more robust roll-out to more DoD activities and agencies. Within the last stage, a DoD enterprise-wide view would be added to enable senior DoD leader risk decisions.

CONCLUSION

The DoD invests heavily to achieve a technical overmatch with adversaries.[47] Unfortunately, in recent years this overmatch has eroded. Like the 2011 and 2015 strategies before, the 2018 Cyber Strategy lacks the specific vision and actions necessary to reverse this trend.[48] This article urges a strategy and framework implementation to more effectively address insider threats by providing an empirical measure of each user's risk through their actual behaviors. UORS will give the user near-real-time awareness of personal behaviors counter to organizational policy and cybersecurity requirements. This measure will also empower management to target training, remediation, and risk reduction while also allowing decision-makers to determine which user risk-exposed areas, roles, or practices require additional remediation more accurately. As a result, all organizational decision levels will be better able to improve cybersecurity resiliency in the face of an ever-evolving insider threat landscape, thereby collectively strengthening the DoD cybersecurity position and fulfilling the 2018 Cyber Strategy objectives.

NOTES

1. Barack Obama, “Presidential Memorandum: NITP; Minimum Standards for Insider Threat Program” (last modified 2012), https://www.dni.gov/index.php/ic-legal-reference-book/presidential-memorandum-nitp-minimum-standards-for-insider-threat-program, accessed October 30, 2018; Department of Defense, “DoD Directive 5205.16” (September 30, 2014; incorporating Change 2, August 28, 2017), http://www.dtic.mil/whs/directives (accessed October 30, 2018).
2. Department of Defense, “Assessment of the Military Services Insider Threat Programs (Redacted)” (2018), https://ogis.archives.gov/, accessed October 2, 2018, 5.
3. Department of Defense, "Summary, DOD Cyber Strategy 2018" (Washington, DC, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, accessed October 2, 2018, 5.
4. U.S. Department of Defense, 2018, 3.
5. Charles Pfleeger, Shari Pfleeger, and Jonathan Margulies, “Security in Computing 5th Edition” (Upper Saddle River, NJ: Prentice Hall, 2015), 474.
6. Jovi Umawing, “The Enemy Is Us: A Look at Insider Threats - Security Boulevard” (last modified 2018), https://securityboulevard.com/2018/08/the-enemy-is-us-a-look-at-insider-threats/, accessed October 2, 2018.
7. Sarah Miller, “Insiders and Their Significant Others: Collusion, Motive and Concealmen” CMU SEI Insights Insider Threat Blog, last modified 2018, https://insights.sei.cmu.edu/insider-threat/2018/04/insiders-and-their-significant-others-collusion-motive-and-concealment.html, accessed October 2, 2018.
8. Department of Defense, “Assessment of the Military Services Insider Threat Programs (Redacted),” 10.
9. Obama, “Presidential Memorandum: NITP; Minimum Standards for Insider Threat Program”; John Thune, “Thune Introduces Legislation to Improve Cybersecurity Resources for Small Businesses - Press Releases - U.S. Senator John Thune” (Hon. John Thune Press Releases, last modified 2017), https://www.thune.senate.gov/public/index.cfm/2017/3/thune-introduces-legislation-to-improve-cybersecurity-resources-for-small-businesses, accessed October 2, 2018; Peter King, "Text - H.R.666 - 115th Congress (2017-2018): Department of Homeland Security Insider Threat and Mitigation Act of 2017" (Washington, DC: U.S. House of Representatives, 2017), https://www.congress.gov/bill/115th-congress/house-bill/666/text, accessed October 2, 2018.
10. Josh Rogin, “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History’ – Foreign Policy” July 9, 2012, , https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/, accessed October 3, 2018.
11. Fran Howarth, “The Role of Human Error in Successful Security Attacks,” IBM Security Intelligence, 2014, https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/, accessed October 2, 2018.
12. Ryan West et al. "Chapter IV The Weakest Link: A Psychological Perspective of Why Users Make Poor Security Decisions," In Social and Human Elements of Information Security: Emerging Trends and Countermeasures, by Manish Gupta and Raj Sharman, (Hershey, PA: Information Science Reference, 2009), http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.467.3395&rep=rep1&type=pdf, 43-60.
13. GAO, “GAO Issues Report on DOD Civilian, Contractor Workforces” (last modified 2018), https://www.gao.gov/products/GAO-18-399, accessed October 2, 2018, i.
14. Russell Rumbaugh and Heidi Peters, “Defense Primer: DOD Contractors” (2017), https://fas.org/sgp/crs/natsec/IF10600.pdf, accessed October 2, 2018, 1.
15. Department of Defense, “About Department of Defense,” US Department of Defense, (last modified 2016), https://dod.defense.gov/about/, accessed October 2, 2018.
16. Varonis, “98 Must-Know Data Breach Statistics for 2021” (2021), https://www.varonis.com/blog/data-breach-statistics/ accessed June 8, 2021; Verizon, “Verizon 2021 Data Breach Investigations Report” (2021), https://verizon.com/dbir/, accessed June 8, 2021.
17. Department of Defense, "Summary, DOD Cyber Strategy 2018," 3.
18. Pfleeger, “Security in Computing 5th Edition,” 31.
19. Bernard Jones, “Overview DOD Defense in Depth Strategy” (no. Security 401 2005), https://www.giac.org/paper/gsec/3907/introduction-computer-security-incident-response/106281, accessed October 2, 2018, 2-9; Dennis E. Shasha, “Defense in Depth,” Scientific American (286, no. 5 (2002)), http://www.nature.com.mutex.gmu.edu/scientificamerican/journal/v286/n5/pdf/scientificamerican0502-101.pdf, accessed September 28, 2018, 101-101; Tim Bass and Roger Robichaux, “Defense-in-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations,” Military Communications Conference (MILCOM 2001, Communications for Network-Centric Operations: Creating the Information Force, IEEE 1, 2001), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=985765, accessed March 23, 2014, 64-70.

NOTES

20. Jared Serbu, “Pentagon Plans New Estimates on Cost, Extent of Its Joint Information Environment,” Federal News Radio (last modified 2016), https://federalnewsradio.com/defense/2016/07/pentagon-plans-new-estimates-cost-extent-joint-information-environment/ , accessed October 2, 2018; The White House, “(FY2018 Budget). INFORMATION TECHNOLOGY Table 16-1. FEDERAL IT SPENDING (2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_16_it.pdf, accessed October 31, 2018.
21. Shane Schick, “Insider Threats Account for Nearly 75 Percent of Security Breach Incidents,” Security Intelligence (last modified 2017), https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/, accessed July 25, 2018; The Council of Economic Advisers, “The Cost of Malicious Cyber Activity to the U.S. Economy” (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, accessed October 3, 2018.
22. Jongwoo Kim, Eun Hee Park, and Richard L. Baskerville, “A Model of Emotion and Computer Abuse,” Information and Management (53, no. 1 (2016)), https://ac-els-cdn-com.mutex.gmu.edu/S0378720615001019/1-s2.0-S0378720615001019-main.pdf?_tid=36a79597-4d34-45ff-8b94-aef28f9432d6&acdnat=1541043735_c5aa52fe-004188935237a18937bcd25f, accessed September 23, 2016, 91-108; Nader Sohrabi Safa and Carsten Maple, “Human Errors in the Information Security Realm – and How to Fix Them,” Computer Fraud and Security (2016, no. 9 (2016)), https://www.sciencedirect.com/science/article/pii/S1361372316300732?via%3Dihub, accessed October 13, 2017, 17-20; Paul van Schaik et al., “Risk Perceptions of Cyber-Security and Precautionary Behaviour,” Computers in Human Behavior (75 (2017)), https://ac-els-cdn-com.mutex.gmu.edu/S074756321730359X/1-s2.0-S074756321730359X-main.pdf?_tid=3bffb04b-1ae8-4071-b46a-322e1d7dddf4&acdnat=1541044749_2487dff92c2a072cfd34301bc4ed3734, accessed January 13, 2018, 554-559; Zinta S. Byrne et al., “From the User’s Perspective: Perceptions of Risk Relative to Benefit Associated with Using the Internet,” Computers in Human Behavior (59 (2016)), https://ac-els-cdn-com.mutex.gmu.edu/S0747563216300760/1-s2.0-S0747563216300760-main.pdf?_tid=7b7bdbc8-bd04-448e-a394-89fec64b7b67&acdnat=1541044970_2dc16d1826bf3e563e026b86bf4e1557, accessed August 13, 2016, 461-468.
23. Dr. Stephen A. Roberts, "Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors," Proquest Dissertations and Theses (Northcentral University, 2021), https://www.proquest.com/openview/c1c31d84698165e5843133986323a773, accessed Jan 30, 2021; Michele Maasberg and Nicole L. Beebe, “The Enemy Within the Insider: Detecting the Insider Threat Through Addiction Theory,” Journal of Information Privacy and Security (10, no. 2 (2014)), https://search-proquest-com.mutex.gmu.edu/docview/1691010505?OpenUrlRefId=info:xri/sid:primo&accountid=14541, accessed September 2, 2017, 59-70; Jeffrey L. Jenkins, “Alleviating Insider Threats: Mitigation Strategies and Detection Techniques,” ProQuest Dissertations and Theses (The University of Arizona, 2013), https://search-proquest-com.mutex.gmu.edu/docview/1426647010/?pq-origsite=primo, accessed December 8, 2015; Asmaa Munshi, Peter Dell, and Helen Armstrong, “Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents,” in Proceedings of the Annual Hawaii International Conference on System Sciences, (2012), https://ieeexplore-ieee-org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=6149306, accessed October 2, 2018, 2402-2411.
24. Tracey Caldwell. “Making Security Awareness Training Work.” Computer Fraud & Security, (2016) https://ac-els-cdn-com.mutex.gmu.edu/S1361372315300464/1-s2.0-S1361372315300464-main.pdf?_tid=ae87b157-7199-4684-85db-b17f-710d43eb&acdnat=1541046318_a057a6f4bb396062a9dd7d4218983812, accessed October 3, 2018, 11-14.
25. Department of Defense, "Summary, DOD Cyber Strategy 2018," 3.
26. Caldwell, “Making Security Awareness Training Work,” 11-14; Mete Eminağoğu, Erdem Uçar, and Şaban Eren, “The Positive Outcomes of Information Security Awareness Training in Companies - A Case Study,” Information Security Technical Report (14, no. 4 (2009)), https://ac-els-cdn-com.mutex.gmu.edu/S1363412710000099/1-s2.0-S1363412710000099-main.pdf?_tid=75c46074-a3c0-4729-9625-86e940a5f01c&acdnat=1541046783_15b690c3eacbefc84cab970c8d5e3b4e, accessed October 2, 2018, 223-229; Steven Furnell and Ismini Vasileiou, “Security Education and Awareness: Just Let Them Burn?,” Network Security (no. 12 (2017), https://ac-els-cdn-com.mutex.gmu.edu/S1353485817301228/1-s2.0-S1353485817301228-main.pdf?_tid=d7e8391e-bd53-4a5b-b251-c2614ba3b1c9&acdnat=1541046892_c6c1f9cb2f9043df-9cb75a23c49d1fe1, accessed October 3, 2018, 5-9.
27. Lijiao Cheng et al., “Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory,” Computers and Security, (39, no. PART B (2013)), https://ac-els-cdn-com.mutex.gmu.edu/S0167404813001387/1-s2.0-S0167404813001387-main.pdf?_tid=d2d699b5-7d55-4a16-becb-5c17e6744d02&acdnat=1541047122_926c2acae1d0290d8cb94d7f931c3c84 ,accessed October 13, 2018, 447-459.
28. Caldwell, “Making Security Awareness Training Work,” 11-14.

NOTES

29. FICO, “Anatomy of a Security Rating” (2018), https://www.fico.com/en/latest-thinking/infographic/anatomy-of-a-security-rating, accessed September 13, 2018.

30. CapitalOne, “Free Credit Score; Report Check with CreditWise - Capital One,” https://creditwise.capitalone.com/home , accessed October 3, 2018.

31. Tatiana Homonoff, Rourke O’Brien, and Abigail Sussman, “Does Knowing Your FICO Score Change Financial Behavior?” Evidence from a Field Experiment with Student Loan Borrowers (SSRN, 2018), https://wagner.nyu.edu/files/faculty/publications/Homonoff%2C O%27Brien%2C and Sussman 2-23-17.pdf , accessed October 3, 2018, 22-24.

32. CapitalOne, “Free Credit Score; Report Check with CreditWise - Capital One”.

33. Homonoff, “Does Knowing Your FICO Score Change Financial Behavior?” 22-24.

34. Society for Human Resource Management, “2017 Talent Acquisition Benchmarking Report” (2017), https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/Documents/2017-Talent-Acquisition-Benchmarking.pdf, accessed January 27, 2019, 4, 9, 13, 15; Aleks Peterson. “Hidden Costs of Onboarding a New Employee” (2018), https://www.glassdoor.com/employers/blog/hidden-costs-employee-onboarding-reduce/, accessed January 28, 2019.

35. Dori Meinert, “Why Trust Matters at Work”(2018), https://www.shrm.org/hr-today/news/hr-magazine/0618/pages/why-trust-matters-at-work.aspx, accessed January 27, 2019); Paul Towers, “Workplace Trust: Why Trust Is Important In The Workplace,” (2017), https://blog.taskpigeon.co/workplace-trust-trust-important-workplace/, accessed January 27, 2019.

36. Society for Human Resource Management, “2017 Talent Acquisition Benchmarking Report”; Clover, “Enterprise behavior: Reduce the cost of employee onboarding” (2018), http://blog.clover.com/better-business/enterprise-behavior-reduce-the-cost-of-employee-on-boarding/, accessed January 28, 2019; Aleks Peterson. “Hidden Costs of Onboarding a New Employee”; Andrew Mcllvaine, “Does new-hire onboarding take too long—or not long enough?” (2018), http://hrexecutive.com/curing-onboardings-ailments/, accessed January 28, 2019.

37. Dell Technologies & Intel, “Data breaches cost US businesses $7M - Business Insider” (2017), http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4, accessed March 6, 2018; IBM & Ponemon Institute, “Cost of a Data Breach Dropped 10 Percent Globally in 2017 Study” (2017), https://www.prnewswire.com/news-releases/ibm--ponemon-institute-cost-of-a-data-breach-dropped-10-percent-globally-in-2017-study-300476378.html, accessed January 28, 2019; Broadcom, “OPM Breach Costs Could Exceed $1 Billion”(2017), https://community.broadcom.com/groups/communities/community-home/librarydocuments/viewdocument?DocumentKey=ea860f79-10aa-4707-870c-6f0ef1cdd3da&CommunityKey=638e24fb-cc43-455a-9185-c8a0130c2076&tab=librarydocuments, accessed June 10, 2021.

38. N. Davinson & E. Sillence, “It won’t happen to me: Promoting secure behaviour among internet users”, Computers in Human Behavior, (26(6), 2010). https://doi.org/10.1016/j.chb.2010.06.023 , accessed January 27, 2019, 1739-1747; V. Dutt, Y.S. Ahn, & C. Gonzalez, “Cyber Situation Awareness,” Human Factors: The Journal of the Human Factors and Ergonomics Society, (55(3), 2013), https://doi.org/10.1177/0018720812464045 , accessed January 27, 2019, 605-618; L. Tomczyk & K. Kopecký, “Children and youth safety on the Internet: Experiences from Czech Republic and Poland,” Telematics and Informatics, (33(3), 2016), https://doi.org/10.1016/j.tele.2015.12.003, accessed January 27, 2019, 822-833.

39. S. Boyson, T. Corsi, & H. Mann, The Cyber Risk Predictive Analytics Project: A NIST and GSA Sponsored Project Principal Investigators (2017), https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/UMD Final Report-Cyber Risk Analytics Project revised tc november 25 2017.pdf, accessed January 28, 2019.

40. L. Neely, “Endpoint Protection and Response: A SANS Survey;” SANS Institute Survey (2018), www.sans.org/reading-room/whitepapers/analyst/next-gen-yet-state-endpoint-security-36827, accessed January 28, 2019.

41. Verizon, “2016 Data Breach Investigations Report”, Verizon Business Journal, (1, 2016), https://doi.org/10.1017/CBO9781107415324.004, accessed January 28, 2019, 1-65.

42. M.L. Collins et al., Common Sense Guide to Mitigating Insider Threats. 5th Edition (December 2016), https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf, accessed January 28, 2019, xii, 6, 11-123.

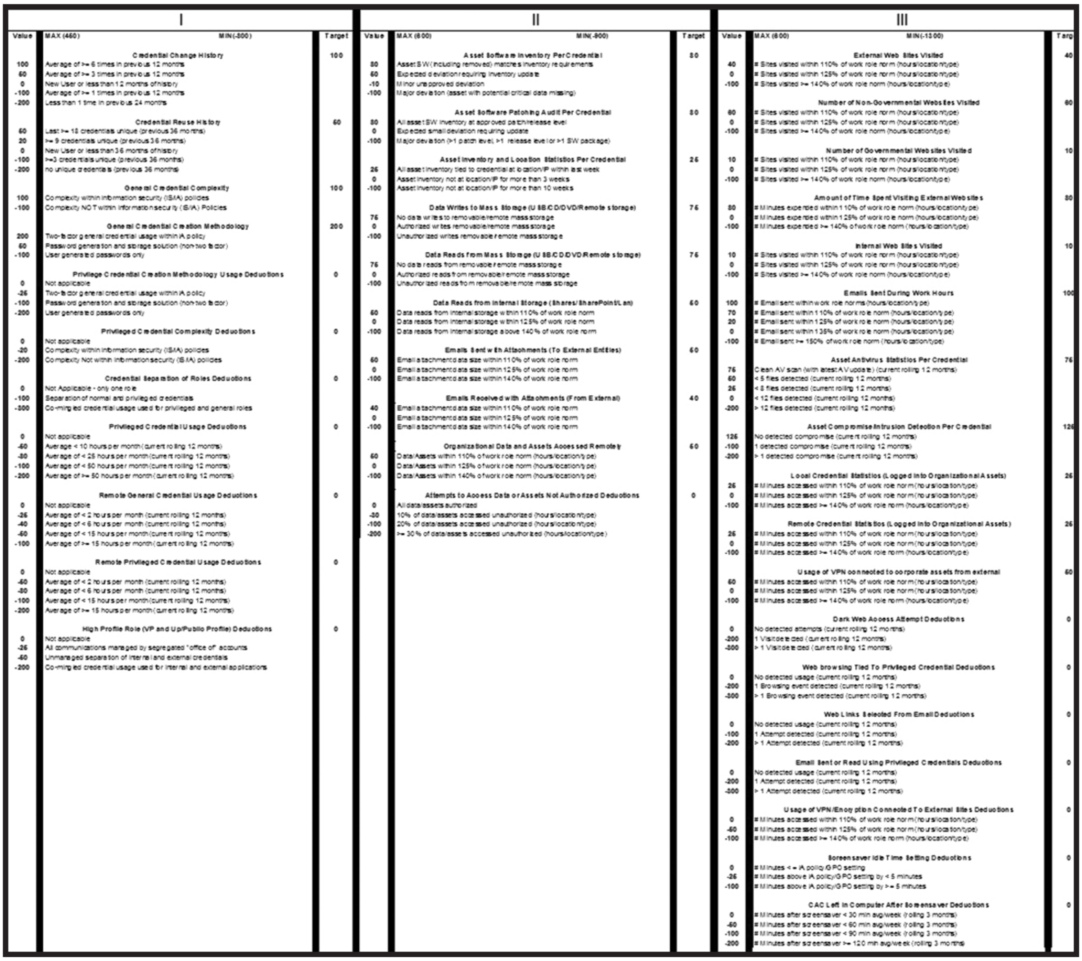
43. H.L. Chou & C. Chou, “An analysis of multiple factors relating to teachers’ problematic information security behavior,” Computers in Human Behavior, (65, 2016), https://doi.org/10.1016/j.chb.2016.08.034, accessed January 28, 2019, 334-345.

44. G.E. Miller, “The U.S. is the Most Overworked Nation in the World,” (2018), https://20somethingfinance.com/american-hours-worked-productivity-vacation/ , accessed January 28, 2019; Sarah Carmichael, “The Research Is Clear: Long Hours Backfire for People and for Companies” (2015), https://hbr.org/2015/08/the-research-is-clear-long-hours-backfire-for-people-and-for-companies, accessed January 28, 2019.

NOTES

45. Ibid: Leslie Perlow & Jessica Porter, “Making Time Off Predictable and Required,” HarvardBusinessReview (2019), http://web.b.ebscohost.com.mutex.gmu.edu/bsi/pdfviewer/pdfviewer?vid=1&sid=f4101167-14b8-4ce4-97a3-504d004fe56e%-40sessionmgr120 , accessed January 28, 2019.
46. M.L. Collins et al. (2016), Common Sense Guide to Mitigating Insider Threats, 5th Edition (December 2016), xii, 6, 11-123.
47. Department of Defense, "Summary, DOD Cyber Strategy 2018," 3.
48. Ibid.; Department of Defense, “DoD Cyber Security Strategy” (2015), http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (accessed October 2, 2018); Department of Defense, "Strategy for Operating in Cyberspace" (2011), http://books.google.com/books?hl=en&lr=&id=YTOY2jPXoiQC&oi=fnd&pg=PA1&dq=Department+of+Defense+Strategy+for+Operating+in+Cyberspace&ots=KJvSm-cJYb&sig=LBdHoKpQlvqRzkb8zIGrVmRScEo, accessed October 8, 2014.

ANNEX A – *UORS Detail Scoring Charts*

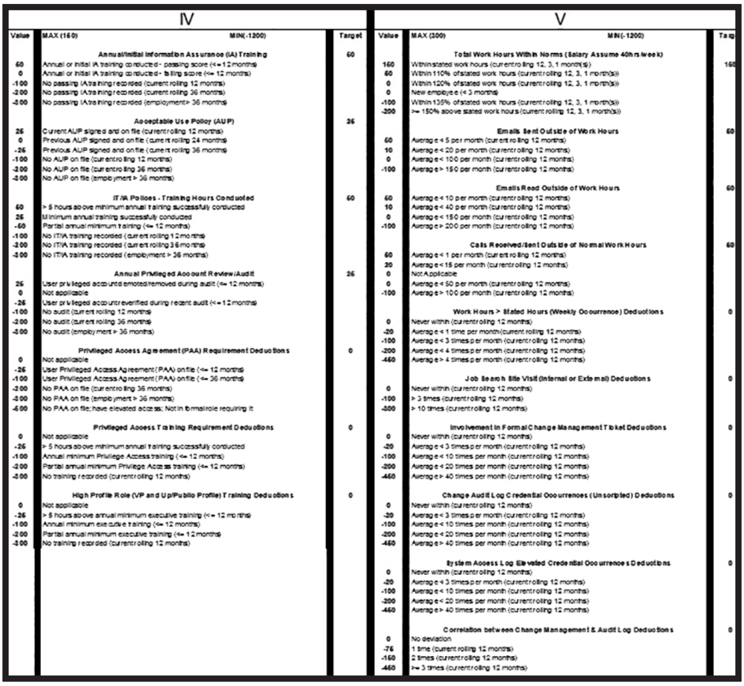


I		
Value	MAX (460) MIN(-800)	Target
	Credential Change History	100
100	Average of >= 6 times in previous 12 months	
50	Average of >= 3 times in previous 12 months	
0	New User or less than 12 months of history	
-100	Average of >= 1 times in previous 12 months	
-200	Less than 1 time in previous 24 months	
	Credential Reuse History	60
60	Last >= 18 credentials unique (previous 36 months)	
20	>= 9 credentials unique (previous 36 months)	
0	New User or less than 36 months of history	
-100	>=3 credentials unique (previous 36 months)	
-200	no unique credentials (previous 36 months)	
	General Credential Complexity	100
100	Complexity within information security (IS/IA) policies	
-100	Complexity NOT within information security (IS/IA) Policies	
	General Credential Creation Methodology	200
200	Two-factor general credential usage within IA policy	
50	Password generation and storage solution (non-two factor)	
-100	User generated passwords only	
	Privilege Credential Creation Methodology Usage Deductions	0
0	Not applicable	
-25	Two-factor general credential usage within IA policy	
-100	Password generation and storage solution (non-two factor)	
-200	User generated passwords only	
	Privileged Credential Complexity Deductions	0
0	Not applicable	
-20	Complexity within information security (IS/IA) policies	
-200	Complexity Not within information security (IS/IA) policies	
	Credential Separation of Roles Deductions	0
0	Not Applicable - only one role	
-100	Separation of normal and privileged credentials	
-300	Co-mingled credential usage used for privileged and general roles	
	Privileged Credential Usage Deductions	0
0	Not applicable	
-60	Average < 10 hours per month (current rolling 12 months)	
-80	Average of < 25 hours per month (current rolling 12 months)	
-100	Average of < 50 hours per month (current rolling 12 months)	
-200	Average of >= 50 hours per month (current rolling 12 months)	
	Remote General Credential Usage Deductions	0
0	Not applicable	
-25	Average of < 2 hours per month (current rolling 12 months)	
-40	Average of < 6 hours per month (current rolling 12 months)	
-60	Average of < 15 hours per month (current rolling 12 months)	
-100	Average of >= 15 hours per month (current rolling 12 months)	
	Remote Privileged Credential Usage Deductions	0
0	Not applicable	
-60	Average of < 2 hours per month (current rolling 12 months)	
-80	Average of < 6 hours per month (current rolling 12 months)	
-100	Average of < 15 hours per month (current rolling 12 months)	
-200	Average of >= 15 hours per month (current rolling 12 months)	
	High Profile Role (VP and Up/Public Profile) Deductions	0
0	Not applicable	
-25	All communications managed by segregated "office of" accounts	
-60	Unmanaged separation of internal and external credentials	
-200	Co-mingled credential usage used for internal and external applications	

II		
Value	MAX (600) MIN(-900)	Target
	Asset Software Inventory Per Credential	80
80	Asset SW (including removed) matches inventory requirements	
60	Expected deviation requiring inventory update	
-10	Minor unapproved deviation	
-100	Major deviation (asset with potential critical data missing)	
	Asset Software Patching Audit Per Credential	80
80	All asset SW inventory at approved patch/release level	
0	Expected small deviation requiring update	
-100	Major deviation (>1 patch level, >1 release level or >1 SW package)	
	Asset Inventory and Location Statistics Per Credential	25
25	All asset inventory tied to credential at location/IP within last week	
0	Asset inventory not at location/IP for more than 3 weeks	
-100	Asset inventory not at location/IP for more than 10 weeks	
	Data Writes to Mass Storage (USB/CD/DVD/Remote storage)	75
75	No data writes to removable/remote mass storage	
0	Authorized writes removable/remote mass storage	
-100	Unauthorized writes removable/remote mass storage	
	Data Reads from Mass Storage (USB/CD/DVD/Remote storage)	75
75	No data reads from removable/remote mass storage	
0	Authorized reads from removable/remote mass storage	
-100	Unauthorized reads from removable/remote mass storage	
	Data Reads from Internal Storage (Shares/SharePoint/Lan)	60
60	Data reads from internal storage within 110% of work role norm	
0	Data reads from internal storage within 125% of work role norm	
-100	Data reads from internal storage above 140% of work role norm	
	Emails Sent with Attachments (To External Entities)	60
60	Email attachment data size within 110% of work role norm	
0	Email attachment data size within 125% of work role norm	
-100	Email attachment data size within 140% of work role norm	
	Emails Received with Attachments (From External)	40
40	Email attachment data size within 110% of work role norm	
0	Email attachment data size within 125% of work role norm	
-100	Email attachment data size within 140% of work role norm	
	Organizational Data and Assets Accessed Remotely	60
60	Data/Assets within 110% of work role norm (hours/location/type)	
0	Data/Assets within 125% of work role norm (hours/location/type)	
-100	Data/Assets within 140% of work role norm (hours/location/type)	
	Attempts to Access Data or Assets Not Authorized Deductions	0
0	All data/assets authorized	
-30	10% of data/assets accessed unauthorized (hours/location/type)	
-100	20% of data/assets accessed unauthorized (hours/location/type)	
-200	>= 30% of data/assets accessed unauthorized (hours/location/type)	

III		
Value	MAX (600) MIN(-1300)	Target
	External Web Sites Visited	40
40	# Sites visited within 110% of work role norm (hours/location/type)	
0	# Sites visited within 125% of work role norm (hours/location/type)	
-100	# Sites visited >= 140% of work role norm (hours/location/type)	
	Number of Non-Governmental Websites Visited	60
60	# Sites visited within 110% of work role norm (hours/location/type)	
0	# Sites visited within 125% of work role norm (hours/location/type)	
-100	# Sites visited >= 140% of work role norm (hours/location/type)	
	Number of Governmental Websites Visited	10
10	# Sites visited within 110% of work role norm (hours/location/type)	
0	# Sites visited within 125% of work role norm (hours/location/type)	
-100	# Sites visited >= 140% of work role norm (hours/location/type)	
	Amount of Time Spent Visiting External Websites	80
80	# Minutes expended within 110% of work role norm (hours/location/type)	
0	# Minutes expended within 125% of work role norm (hours/location/type)	
-100	# Minutes expended >= 140% of work role norm (hours/location/type)	
	Internal Web Sites Visited	10
10	# Sites visited within 110% of work role norm (hours/location/type)	
0	# Sites visited within 125% of work role norm (hours/location/type)	
-100	# Sites visited >= 140% of work role norm (hours/location/type)	
	Emails Sent During Work Hours	100
100	# Email sent within work role norms (hours/location/type)	
70	# Email sent within 110% of work role norm (hours/location/type)	
20	# Email sent within 125% of work role norm (hours/location/type)	
0	# Email sent within 135% of work role norm (hours/location/type)	
-100	# Email sent >= 150% of work role norm (hours/location/type)	
	Asset Antivirus Statistics Per Credential	75
75	Clean AV scan (with latest AV update) (current rolling 12 months)	
50	< 5 files detected (current rolling 12 months)	
25	< 8 files detected (current rolling 12 months)	
0	< 12 files detected (current rolling 12 months)	
-200	> 12 files detected (current rolling 12 months)	
	Asset Compromise/Intrusion Detection Per Credential	125
125	No detected compromise (current rolling 12 months)	
-100	1 detected compromise (current rolling 12 months)	
-200	> 1 detected compromise (current rolling 12 months)	
	Local Credential Statistics (Logged into Organizational Assets)	25
25	# Minutes accessed within 110% of work role norm (hours/location/type)	
0	# Minutes accessed within 125% of work role norm (hours/location/type)	
-100	# Minutes accessed >= 140% of work role norm (hours/location/type)	
	Remote Credential Statistics (Logged into Organizational Assets)	25
25	# Minutes accessed within 110% of work role norm (hours/location/type)	
0	# Minutes accessed within 125% of work role norm (hours/location/type)	
-100	# Minutes accessed >= 140% of work role norm (hours/location/type)	
	Usage of VPN connected to corporate assets from external	60
60	# Minutes accessed within 110% of work role norm (hours/location/type)	
0	# Minutes accessed within 125% of work role norm (hours/location/type)	
-100	# Minutes accessed >= 140% of work role norm (hours/location/type)	
	Dark Web Access Attempt Deductions	0
0	No detected attempts (current rolling 12 months)	
-200	1 Visit detected (current rolling 12 months)	
-300	> 1 Visit detected (current rolling 12 months)	
	Web browsing Tied To Privileged Credential Deductions	0
0	No detected usage (current rolling 12 months)	
-200	1 Browsing event detected (current rolling 12 months)	
-300	> 1 Browsing event detected (current rolling 12 months)	
	Web Links Selected From Email Deductions	0
0	No detected usage (current rolling 12 months)	
-100	1 Attempt detected (current rolling 12 months)	
-200	> 1 Attempt detected (current rolling 12 months)	
	Email Sent or Read Using Privileged Credentials Deductions	0
0	No detected usage (current rolling 12 months)	
-200	1 Attempt detected (current rolling 12 months)	
-300	> 1 Attempt detected (current rolling 12 months)	
	Usage of VPN/Encryption Connected To External Sites Deductions	0
0	# Minutes accessed within 110% of work role norm (hours/location/type)	
-60	# Minutes accessed within 125% of work role norm (hours/location/type)	
-100	# Minutes accessed >= 140% of work role norm (hours/location/type)	
	Screensaver Idle Time Setting Deductions	0
0	# Minutes <= IA policy/GPO setting	
-25	# Minutes above IA policy/GPO setting by < 5 minutes	
-100	# Minutes above IA policy/GPO setting by >= 5 minutes	
	CAC Left in Computer After Screensaver Deductions	0
0	# Minutes after screensaver < 30 min avg/week (rolling 3 months)	
-60	# Minutes after screensaver < 60 min avg/week (rolling 3 months)	
-100	# Minutes after screensaver < 90 min avg/week (rolling 3 months)	
-200	# Minutes after screensaver >= 120 min avg/week (rolling 3 months)	

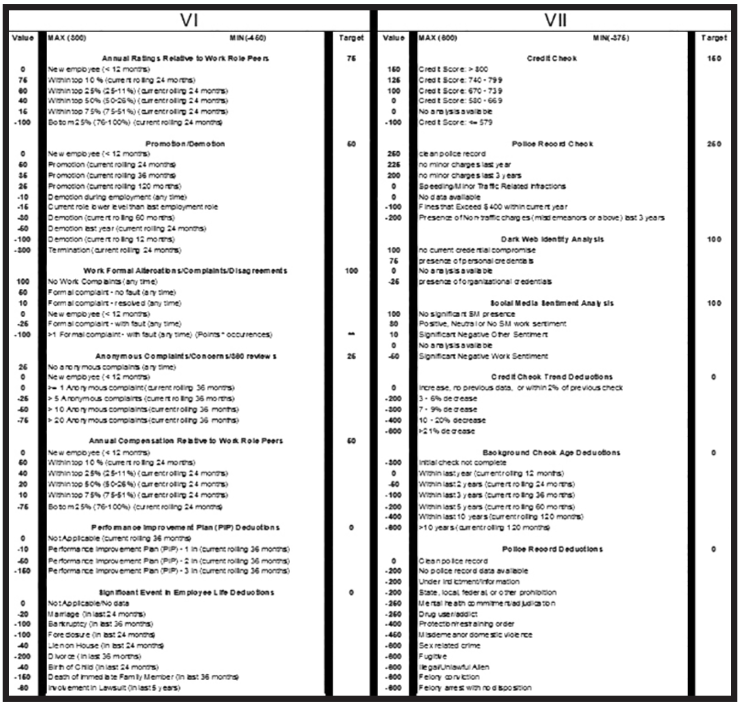
Figure 2. UORS Categories I, II, & III Scoring



IV		
Value	MAX (150) MIN(-1200)	Target
	Annual/Initial Information Assurance (IA) Training	50
50	Annual or initial IA training conducted - passing score (<= 12 months)	
0	Annual or initial IA training conducted - failing score (<= 12 months)	
-100	No passing IA training recorded (current rolling 12 months)	
-200	No passing IA training recorded (current rolling 36 months)	
-300	No passing IA training recorded (employment> 36 months)	
	Acceptable Use Policy (AUP)	25
25	Current AUP signed and on file (current rolling 12 months)	
0	Previous AUP signed and on file (current rolling 24 months)	
-25	Previous AUP signed and on file (current rolling 36 months)	
-100	No AUP on file (current rolling 12 months)	
-200	No AUP on file (current rolling 36 months)	
-300	No AUP on file (employment > 36 months)	
	IT/IA Policies - Training Hours Conducted	50
50	> 5 hours above minimum annual training successfully conducted	
25	Minimum annual training successfully conducted	
-50	Partial annual minimum training (<= 12 months)	
-100	No IT/IA training recorded (current rolling 12 months)	
-200	No IT/IA training recorded (current rolling 36 months)	
-300	No IT/IA training recorded (employment > 36 months)	
	Annual Privileged Account Review/Audit	25
25	User privileged account demoted/removed during audit (<= 12 months)	
0	Not applicable	
-25	User privileged account reverified during recent audit (<= 12 months)	
-100	No audit (current rolling 12 months)	
-200	No audit (current rolling 36 months)	
-300	No audit (employment > 36 months)	
	Privileged Access Agreement (PAA) Requirement Deductions	0
0	Not applicable	
-25	User Privileged Access Agreement (PAA) on file (<= 12 months)	
-100	User Privileged Access Agreement (PAA) on file (<= 36 months)	
-200	No PAA on file (current rolling 36 months)	
-300	No PAA on file (employment > 36 months)	
-500	No PAA on file; have elevated access; Not in formal role requiring it	
	Privileged Access Training Requirement Deductions	0
0	Not applicable	
-25	> 5 hours above minimum annual training successfully conducted	
-100	Annual minimum Privilege Access training (<= 12 months)	
-200	Partial annual minimum Privilege Access training (<= 12 months)	
-300	No training recorded (current rolling 12 months)	
	High Profile Role (VP and Up/Public Profile) Training Deductions	0
0	Not applicable	
-25	> 5 hours above annual minimum executive training (<= 12 months)	
-100	Annual minimum executive training (<= 12 months)	
-200	Partial annual minimum executive training (<= 12 months)	
-300	No training recorded (current rolling 12 months)	

V		
Value	MAX (300) MIN(-1200)	Target
	Total Work Hours Within Norms (Salary Assume 40hrs/week)	150
150	Within stated work hours (current rolling 12, 3, 1 month(s))	
50	Within 110% of stated work hours (current rolling 12, 3, 1 month(s))	
0	Within 120% of stated work hours (current rolling 12, 3, 1 month(s))	
0	New employee (< 3 months)	
-100	Within 135% of stated work hours (current rolling 12, 3, 1 month(s))	
-200	>= 150% above stated work hours (current rolling 12, 3, 1 month(s))	
	Emails Sent Outside of Work Hours	50
50	Average < 5 per month (current rolling 12 months)	
10	Average < 20 per month (current rolling 12 months)	
0	Average < 100 per month (current rolling 12 months)	
-100	Average > 150 per month (current rolling 12 months)	
	Emails Read Outside of Work Hours	50
50	Average < 10 per month (current rolling 12 months)	
10	Average < 40 per month (current rolling 12 months)	
0	Average < 150 per month (current rolling 12 months)	
-100	Average > 200 per month (current rolling 12 months)	
	Calls Received/Sent Outside of Normal Work Hours	50
50	Average < 1 per month (current rolling 12 months)	
20	Average < 15 per month (current rolling 12 months)	
0	Not Applicable	
0	Average < 50 per month (current rolling 12 months)	
-100	Average > 100 per month (current rolling 12 months)	
	Work Hours > Stated Hours (Weekly Occurrence) Deductions	0
0	Never within (current rolling 12 months)	
-20	Average < 1 time per month(current rolling 12 months)	
-100	Average < 3 times per month (current rolling 12 months)	
-200	Average < 4 times per month (current rolling 12 months)	
-450	Average > 4 times per month (current rolling 12 months)	
	Job Search Site Visit (Internal or External) Deductions	0
0	Never within (current rolling 12 months)	
-100	> 3 times (current rolling 12 months)	
-300	> 10 times (current rolling 12 months)	
	Involvement in Formal Change Management Ticket Deductions	0
0	Never within (current rolling 12 months)	
-20	Average < 3 times per month (current rolling 12 months)	
-100	Average < 10 times per month (current rolling 12 months)	
-200	Average < 20 times per month (current rolling 12 months)	
-450	Average > 40 times per month (current rolling 12 months)	
	Change Audit Log Credential Occurrences (Unscripted) Deductions	0
0	Never within (current rolling 12 months)	
-20	Average < 3 times per month (current rolling 12 months)	
-100	Average < 10 times per month (current rolling 12 months)	
-200	Average < 20 times per month (current rolling 12 months)	
-450	Average > 40 times per month (current rolling 12 months)	
	System Access Log Elevated Credential Occurrences Deductions	0
0	Never within (current rolling 12 months)	
-20	Average < 3 times per month (current rolling 12 months)	
-100	Average < 10 times per month (current rolling 12 months)	
-200	Average < 20 times per month (current rolling 12 months)	
-450	Average > 40 times per month (current rolling 12 months)	
	Correlation between Change Management & Audit Log Deductions	0
0	No deviation	
-75	1 time (current rolling 12 months)	
-150	2 times (current rolling 12 months)	
-450	>= 3 times (current rolling 12 months)	

Figure 3. UORS Categories IV & V Scoring



VI		
Value	MAX (300) MIN(-450)	Target
	Annual Ratings Relative to Work Role Peers	75
0	New employee (< 12 months)	
75	Within top 10 % (current rolling 24 months)	
50	Within top 25% (25-11 %) (current rolling 24 months)	
40	Within top 50% (50-26%) (current rolling 24 months)	
15	Within top 75% (75-51 %) (current rolling 24 months)	
-100	Bottom 25% (76-100%) (current rolling 24 months)	
	Promotion/Demotion	50
0	New employee (< 12 months)	
50	Promotion (current rolling 24 months)	
35	Promotion (current rolling 36 months)	
25	Promotion (current rolling 120 months)	
-10	Demotion during employment (any time)	
-15	Current role lower level than last employment role	
-30	Demotion (current rolling 60 months)	
-50	Demotion last year (current rolling 24 months)	
-100	Demotion (current rolling 12 months)	
-300	Termination (current rolling 24 months)	
	Work Formal Altercations/Complaints/Disagreements	100
100	No Work Complaints (any time)	
50	Formal complaint - no fault (any time)	
10	Formal complaint - resolved (any time)	
0	New employee (< 12 months)	
-25	Formal complaint - with fault (any time)	
-100	>1 Formal complaint - with fault (any time) (Points * occurrences)	**
	Anonymous Complaints/Concerns/360 reviews	25
25	No anonymous complaints (any time)	
0	New employee (< 12 months)	
0	>= 1 Anonymous complaint (current rolling 36 months)	
-25	> 5 Anonymous complaints (current rolling 36 months)	
-50	> 10 Anonymous complaints (current rolling 36 months)	
-75	> 20 Anonymous complaints (current rolling 36 months)	
	Annual Compensation Relative to Work Role Peers	50
0	New employee (< 12 months)	
50	Within top 10 % (current rolling 24 months)	
40	Within top 25% (25-11 %) (current rolling 24 months)	
20	Within top 50% (50-26%) (current rolling 24 months)	
10	Within top 75% (75-51 %) (current rolling 24 months)	
-75	Bottom 25% (76-100%) (current rolling 24 months)	
	Performance Improvement Plan (PIP) Deductions	0
0	Not Applicable (current rolling 36 months)	
-10	Performance Improvement Plan (PIP) - 1 in (current rolling 36 months)	
-50	Performance Improvement Plan (PIP) - 2 in (current rolling 36 months)	
-150	Performance Improvement Plan (PIP) - 3 in (current rolling 36 months)	
	Significant Event in Employee Life Deductions	0
0	Not Applicable/No data	
-20	Marriage (in last 24 months)	
-100	Bankruptcy (in last 36 months)	
-100	Foreclosure (in last 24 months)	
-40	Lien on House (in last 24 months)	
-200	Divorce (in last 36 months)	
-40	Birth of Child (in last 24 months)	
-150	Death of Immediate Family Member (in last 36 months)	
-50	Involvement in Lawsuit (in last 5 years)	

VII		
Value	MAX (600) MIN(-375)	Target
	Credit Check	150
150	Credit Score: > 800	
125	Credit Score: 740 - 799	
100	Credit Score: 670 - 739	
0	Credit Score: 580 - 669	
0	No analysis available	
-100	Credit Score: <= 579	
	Police Record Check	250
250	clean police record	
225	no minor charges last year	
200	no minor charges last 3 years	
0	Speeding/Minor Traffic Related Infractions	
0	No data available	
-100	Fines that Exceed $400 within current year	
-200	Presence of Non-traffic charges (misdemeanors or above) last 3 years	
	Dark Web Identity Analysis	100
100	no current credential compromise	
75	presence of personal credentials	
0	No analysis available	
-25	presence of organizational credentials	
	Social Media Sentiment Analysis	100
100	No significant SM presence	
50	Positive, Neutral or No SM work sentiment	
10	Significant Negative Other Sentiment	
0	No analysis available	
-50	Significant Negative Work Sentiment	
	Credit Check Trend Deductions	0
0	Increase, no previous data, or within 2% of previous check	
-200	3 - 6% decrease	
-300	7 - 9% decrease	
-400	10 - 20% decrease	
-600	>21% decrease	
	Background Check Age Deductions	0
-300	Initial check not complete	
0	Within last year (current rolling 12 months)	
-50	Within last 2 years (current rolling 24 months)	
-100	Within last 3 years (current rolling 36 months)	
-200	Within last 5 years (current rolling 60 months)	
-400	Within last 10 years (current rolling 120 months)	
-600	>10 years (current rolling 120 months)	
	Police Record Deductions	0
0	Clean police record	
-200	No police record data available	
-200	Under indictment/information	
-200	State, local, federal, or other prohibition	
-250	Mental health commitment/adjudication	
-250	Drug user/addict	
-400	Protection/restraining order	
-450	Misdemeanor domestic violence	
-600	Sex related crime	
-600	Fugitive	
-600	Illegal/Unlawful Alien	
-600	Felony conviction	
-600	Felony arrest with no disposition	

Figure 4. UORS Categories VI & VII Scoring