Millennial Considerations on Insider Threat: Are We A Threat Or An Opportunity?

May 2019

Ian Brinksman, Madeline Christian, Desercé Johnston, Garry Stevens, Grace Meany, Aaron Metheny, Colin Neafsey, Erick Plascencia, Sonny Santistevan, Nika Smernoff, Coco Tang, Constantine Venizelos, John Woog

Professors Jeffrey Connor & Carol Rollie Flynn
All statements of fact, opinion, or analysis expressed are those of the authors and do not reflect the opinion of any individual author’s employer and/or the US Government.
A special report prepared by the

NATIONAL SECURITY CRITICAL ISSUES TASK FORCE (NSCITF)

Published by the Georgetown Security Studies Review at the Center for Security Studies at the Georgetown University Edmund A. Walsh School of Foreign Service

Task Force Members:

Ian Brinksman  Grace Meany  Sonny Santistevan
Madeline Christian  Aaron Metheny  Nika Smernoff
Desereé Johnston  Colin Neafsey  Coco Tang
Garry Stevens  Erick Plascencia  Constantine Venizelos

John Woog

Professor Jeffrey Connor
Professor Carol Rollie Flynn

Edited by:

GSSR

Access the Georgetown Security Studies Review online at http://gssr.georgetown.edu
Connect on Facebook at http://www.facebook.com/GeorgetownUniversityGSSR
Follow the Georgetown Security Studies Review on Twitter at ‘@gssreview’
Contact the Editor-in-Chief at GSSR@georgetown.edu

DISCLAIMER

The views expressed in the Georgetown Security Studies Review do not necessarily represent those of the editors or staff of the GSSR, the Edmund A. Walsh School of Foreign Service, or Georgetown University.

The Editorial Board of the GSSR and its affiliated peer reviewers strive to verify the accuracy of all factual information contained in the GSSR. However, the staffs of the GSSR, the Edmund A. Walsh School of Foreign Service, and Georgetown University make no warranties or representations regarding the completeness or accuracy of information contained in the GSSR, and they assume no legal liability or responsibility for the content of any work contained therein. Copyright 2012 – 2018, Georgetown Security Studies Review. All rights reserved.
# TABLE OF CONTENTS

I. ABSTRACT 6

II. EXECUTIVE SUMMARY 7
Summary of Key Findings and Recommendations 7

III. INTENT 9

IV. BACKGROUND and DEFINITIONS 12

V. METHODOLOGY 13

VI. KEY FINDINGS 14
Key Finding 1 14
Key Finding 2 19
Key Finding 3 25
Key Finding 4 30
Key Finding 5 35

VII. RECOMMENDATIONS 39
Recommendation 1 39
Recommendation 2 40
Recommendation 3 42
Recommendation 4 43
Recommendation 5 47

VIII. FINAL THOUGHTS 49

IX. BIBLIOGRAPHY 50
## TABLE OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Task Force Infographic</td>
<td>11</td>
</tr>
<tr>
<td>Figure 2</td>
<td>2016 US population by generation</td>
<td>12</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Pew Research Center surveillance data</td>
<td>18</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Forrester Consulting “Pursuing the Mobile Moment” data</td>
<td>19</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Private sector best practices for government</td>
<td>21</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Comparing traditional and millennial organizational structures</td>
<td>22</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Generational Divide Insider Threat</td>
<td>26</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Generational Engagement at Work</td>
<td>27</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Financial impact of the Great Recession</td>
<td>28</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Device Proliferation</td>
<td>33</td>
</tr>
</tbody>
</table>
I. ABSTRACT

As insider threat prevention receives increasing attention, the National Security Critical Issues Task Force examined if Millennials—now the largest segment of the workforce—represent a threat or an opportunity to employers. Through this research we found that Millennials have the same triggers to become insider threats as previous generations, but have so far engaged in insider threat at much lower rates. Millennials may be susceptible to insider threat in new ways, however, such as unprecedented levels of debt earlier in life, targeting opportunities from social media, and technology vulnerabilities due to mobile device usage. To address these challenges, we examined how various large private sector organizations have adapted their corporate culture to better engage their Millennial workforce. Based on our research and findings, we recommend that employers take a two-pronged approach. First, organizations should make adjustments to the corporate culture to reflect Millennial preferences; examples include flattening the management structure, providing clear pathways to professional development, and prioritizing community engagement. Second, employers should develop a comprehensive insider threat program which educates employees on appropriate social media and mobile device usage, while also monitoring employee behavior and technology advancements that could create new vulnerabilities. Implementing the aforementioned recommendations will not eliminate insider threat completely, but could help reduce it through increased job satisfaction, education, and vigilance.
II. EXECUTIVE SUMMARY

A recent spate of high-profile classified leaks and data breaches\(^1\) has catapulted the specter of insider threat from a holdover of intelligence agencies to one of the top concerns for private and public sector organizations. With technological advancements creating new vulnerabilities and media platforms aiding the dissemination of sensitive information, disgruntled employees have ever more avenues to wreak havoc on their employers.\(^2\) Moreover, as seen with the Snowden revelations, the highly sensitive nature of the information at risk in government poses a very real threat to national security. Keeping employees happy and engaged, then, is a key component of any effective insider threat prevention strategy.\(^3\)

The insider threat phenomenon has created an urgent incentive to adapt organizational policies and cultures to the Millennial generation. In 2015, Millennials - those born between 1980 and 2000 - surpassed Generation X as the dominant generation in the US labor force.\(^4\) With so many Millennial workers, it is crucial for employers to create a satisfying work environment to minimize the instances of insider threat. The imperative to adapt organizational culture will only accelerate as the peak of Millennials in the workforce is still on the horizon; the youngest are just now graduating from high school.

This paper shows that, although Millennial value systems do not differ intrinsically from other generations, factors like formative experiences, intergenerational perspectives, and cultural traumas - such as the fallout from the Great Recession - have created some differences between the generations which further inform organizational changes and technological shifts. These adaptations will become increasingly important to meeting insider threat in the Digital Age.

Leveraging Millennial values increases engagement in the workplace, fostering a more interactive environment and flattening hierarchical management structures. Organizations seeking to minimize the risk of insider threat should reinstate programs that reward employee longevity and provide pathways for professional development; for all of technology’s advantages, there is no substitute for community-building events that promote face-to-face interaction. Organizations can also cater to Millennial desires for workplace flexibility, but must

---

\(^1\) Recent high-profile leaks include Edward Snowden (https://www.theguardian.com/world/2013/jun/23/edward-
\(^3\) Coyne, Michael, interview by authors, January 29, 2018.
remain aware of the increased risk of unintentional security breaches that this flexibility creates. While the addition of devices to a network creates inherent vulnerabilities, there is also the risk that Millennials and future generations’ interaction with technology could exacerbate existing vulnerabilities by creating opportunities for targeting by malicious actors.

The U.S. government can take steps to mitigate these risks through cyber education, legislation that reduces anonymity online and forces employees to confront the professional consequences of their digital behavior, and a public awareness campaign that promotes the positive attributes of an intergenerational workforce. Integrating technology and human factors within a comprehensive set of insider threat policies and procedures will further increase the effectiveness of prevention and detection programs.

This paper proceeds in three parts. The first section provides background information on the Millennial generation regarding overall economic trends, workplace satisfaction, and the prevalence of Millennial insider threat. Next, the second section reviews key findings from studying Millennial psychology, organizational cultures, and the impact of technology on the generation. The paper concludes with recommendations for organizations to better adapt to Millennial culture and to foster a more positive work environment. Implementing these recommendations will not eliminate insider threat completely, but could help reduce it through increased job satisfaction, education, and vigilance.

The following page provides a high-level review of the Task Force’s key findings and recommendations.
KEY FINDINGS

1. Millennial Value Systems Do Not Differ Intrinsically from Other Generations. However, Formative Experiences, Intergenerational Perspectives, and Cultural Traumas Have Generated Distinctive Characteristics. Understanding Millennial Value Systems is Useful for Insider Threat Assessments.

2. Public Sector Organizations Can Leverage Flat Organizational Structures to Promote Millennial Values and Mitigate Insider Threat Risk Factors.

3. Fewer Millennials are Attempting to Harm Their Company Than Members of Other Generations.

4. Millennials’ Workplace Preferences and Device Usage Pose Challenges for Insider Threat Prevention and Detection.

5. Technology Dependency May Reduce Millennials’ Ability to Cope with Professional Stressors and Personal Crises.

RECOMMENDATIONS

1. Private and Public Organizations Should Reinstate Programs that Reward Employee Longevity and Provide Pathways for Professional Development.

2. Organizations Should Prioritize Employee Community-Building Events that Increase Face-to-Face Interaction.


4. Organizations Should Mitigate the Risk of Insider Threat By Implementing a Comprehensive Structure of Policies and Procedures.


III. INTENT

This report endeavors to make a unique contribution to the insider threat discussion by applying generational considerations to insider threat prevention. The task force chose to address generational differences because the preponderance of insider threat analysis focuses on
psychological and situational differences among individuals, often disregarding distinctions between generational cohorts. In 2015, Millennials became the largest workforce demographic. Thus, public and private organizations could immediately benefit from better understanding Millennials. However, most generational literature about Millennials is written from the perspective of other generations. As a result, the term “Millennial” often carries a negative connotation, which can impact individual psyches and employment opportunities. Therefore, our report attempts to counter existing bias. By looking at their collective identity and professional experience, we are able to determine Millennials continue to face great insecurity as individuals, professionals, and Americans.

The task force understands the implementation of its recommendations will not eliminate insider threat completely. Yet, Millennial values and behavior have been altered by diverse experiences, dynamically impacting their workplace desires and satisfaction. The task force believes organizations that better understand their incoming workforce and adapt to generational differences will have greater success in reducing insider threat incidents in the future.

All members of this task force are Millennials, with an average age of twenty-nine years. Each earned a master’s degree in Security Studies from the Georgetown University Walsh School of Foreign Service and resides in the Washington, D.C. metro region. In an effort to further qualify its perspective, the task force members answered forty questions modeled after cross-generational and political surveys conducted by Gallup, Pew Research Center, Deloitte, and Harvard University. A selection of the findings is presented through an infographic below. Its intent is to highlight significant generational differences by allowing readers of this study to compare their life experiences to those of the task force at the same age. The infographic provides data pertaining to the task force members’ homelives, worklives, financial status, technology use, political involvement, and levels of trust in the public and private sectors. Insider threat literature indicates that dissatisfaction in these sectors may lead to vulnerabilities or negative actions by individual employees. Therefore, the task force members participated in this survey to ascertain their own vulnerabilities and outlook as Millennials.

MEET THE TASK FORCE

13 MEMBERS   AVERAGE AGE: 29   5 WOMEN / 8 MEN

MASTER’S IN SECURITY STUDIES
GEORGETOWN UNIVERSITY

60% VOTE IN MIDTERM & PRESIDENTIAL ELECTIONS
46% DON’T TRUST PRIVATE COMPANIES
8% DON’T TRUST GOVERNMENT
46% GENERALLY HOPEFUL ABOUT FUTURE OF THE US

58% LIVE 200+ MILES FROM A RELATIVE
FORTY PERCENT HAVE HAD 3 TO 4 FULL-TIME JOBS SINCE COLLEGE
ZERO ARE MARRIED, OWN A HOME, OR HAVE KIDS

OWN 3+ SMART DEVICES 76%

41% WORK REMOTELY 2-3 DAYS A WEEK

HAD INTERNET AT HOME, AGED 10-12 60%

$43,857 STARTING SALARY (GS-9)

60% PAY $1500+ RENT & HAVE A ROOMMATE

STUDENT DEBT
$1-25K 32% $25-50K 15% $50-75K 15% $100K+ 15%
IV. BACKGROUND AND DEFINITIONS

INSIDER THREAT:

Although insider threat is not a new concern, scholars and practitioners have not reached consensus on a universal definition of the threat. The most common definitions of insider threat incorporate activities such as data leaks, espionage, fraud, intellectual property theft, misuse of computer networks, sabotage, unauthorized dissemination of trade secrets or classified material, and workplace violence. This report uses the definition proffered by Carnegie Mellon University’s Software Engineering Institute which uses adequately broad language to encompass all of these activities:

“An insider threat is the potential for an individual who has or had authorized access to an organization’s assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect their organization.”

MILLENNIAL:

The U.S. Census Bureau and other government organizations typically define societal generations by birth ranges of approximately fifteen year increments. The exact upper and lower bound and ranges used, however, vary from institution to institution and between generational studies. Additionally, generational cohorts are frequently

---


assigned multiple epithets whose definitions overlap, but include subtle differences that cloud uniform consensus. This report defines the millennial generation as those individuals born between 1980 and 2000. “Digital native” is a term that typically refers to those born after 1980 who grew up surrounded by and socialized to digital technology. The report uses this term interchangeably with Millennial, as essentially all Millennials are by definition digital natives. However, the terms are not synonymous as being a digital native is only one, albeit key, component of millennial identity. Moreover, the term is not unique to Millennials as all future generations will also be digital natives.

V. METHODOLOGY

The task force conducted diverse and robust research on insider threat. The research encompassed multiple dimensions of insider threat, including the history of insider attacks, the range of potential threats, the psychology of attackers, organizational leadership and culture, and the technology available to identify and prevent attacks. Members of the task force spent five months conducting literature reviews and interviewing analysts, operators, and leaders in law enforcement, the intelligence community, the diplomatic community, the military, and private industry.

This report benefited from a multi-tiered research approach. First, all thirteen student members provided individual analysis to the final product. Each student analyzed an insider attack and offered insights on the event, addressing the motivation of the attacker and potential preventative measures. Students also interviewed two insider threat experts in the Washington, DC region to better understand current threats and gaps within insider threat literature. The individual perspectives were presented to all members of the task force and influenced the direction of the final report.

The second tier of research was small group analysis. From the comprehensive literature review and the individual contributions, the task force members discovered three overarching research areas: 1) Psychology of Insiders; 2) Organizational Culture’s Relationship to Insider Threat; and 3) Technology Solutions for Insider Threat. The students divided themselves into

---

three focus groups to further explore each area and determine prevention strategies. Each group established priorities, isolated key findings, and crafted recommendations for action.

The group research incorporated academic studies on generations, psychological analysis of insider threats, scholarship on the establishment of values systems, examinations of organizational cultures and their impact on workers, and cross-generational survey data. While all three areas had diverse scholarship, the research drew primarily from qualitative and U.S.-centric sources. This approach is consistent with the task force’s U.S. perspective. The group tier was particularly important because the research focus ultimately shifted from a broad understanding of insider threat to the relationship between Millennials and insider threat.

The full task force completed the third tier of research. Members considered and debated the findings and recommendations of all three group reports. Once a consensus was reached, the group reports were synthesized into one. Then, the task force presented its joint findings to a panel of insider threat experts from the U.S. Government and private industry. During the briefing, task force members addressed questions from attendees and encouraged critique. Following the briefing, the task force incorporated suggestions and finalized its report. The result is this comprehensive report on the current understanding of insider threat in relation to generational cohorts. The report provides analysis and recommendations that are actionable in a variety of organizations, but should not be taken as an exhaustive list of insider threat prevention opportunities. Indeed, there is considerable room for further research on the topic.

VI. KEY FINDINGS

Key Finding 1: Millennial Value Systems Do Not Intrinsically Differ from Other Generations. However, Formative Experiences, Intergenerational Perspectives, and Cultural Traumas Have Generated Distinctive Characteristics. Understanding Millennial Value Systems is Useful for Insider Threat Assessments.

Value systems serve as a foundation for an individual’s conduct. Analyzing these systems in a generational context is especially useful for insider threat assessments, as values help characterize the types of individuals or groups that commit malicious acts. If the typical insider is
a “person in crisis,” then he or she also is prone to having “a severe loss of control.” His or her value system, however, should be instinctual during a crisis. Therefore, understanding the values that should guide decisions and actions during a crisis is important.

Empirical analysis demonstrates that altruistic values do not differ among generations in the United States. A study found that generational variables explained different values 7 percent of the time, a finding deemed significant when compared to all other existing influences. Yet, a lack of quantitative evidence, the lasting impact of negative interactions, and a bias toward one’s own generation fuel misconceptions regarding other generations.

American values generally remain constant over time, with occasional periods of cultural upheaval in response to significant events or social movements. The lasting impact of such periods depends on the timing within a generational lifestyle. Significant events may sufficiently impact generations in their formative years, altering their value system away from the culture, values, and norms into which they were born. For Millennials, the shock and aftermath of the September 11, 2001 terrorist attacks was a cultural trauma reinforced by the widespread “sentiment that the country will never be the same.” While other generations experienced their own cultural trauma (such as the Great Depression, World War II, the JFK assassination, or the Vietnam War), Millennials experienced the trauma in real time and relived the experience constantly through intimate footage and audio recordings on television and the Internet. Continuous exposure of this nature may alter Millennials’ “collective memory,” a term that encompasses a generation’s shared life experience and that generation’s retained memory of the experience.

In addition to the September 11 attacks, other cultural traumas such as the high divorce rate of Millennials’ parents and the Great Recession have significantly influenced Millennial

---

value systems. In 2007, researchers Sean Lyons, Linda Duxbury, and Christopher Higgins published a study on generational differences in human values. The study based its evaluations on the Schwartz Value Survey, involving a typology of ten different value types grouped into four value domains. The study determined that Millennials and Generation X held high “self-enhancement” values–power, achievement, and hedonism–and low “self-transcendence” values–universalism and benevolence as compared to Baby Boomers and Matures (those born before 1945).  

Yet Millennials aligned with the “conservation” values of tradition, conformity, and security more than Generation X. These findings support theories that Millennial value systems are on average more in line with the values of Matures. The result of this study is valuable as it contradicts general stereotypes of Millennials and their outlook Insider threat analysts could benefit from in

"For Millennials, the shock and aftermath of the September 11, 2001 terrorist attacks was a cultural trauma reinforced by the widespread sentiment that the country will never be the same."

The most significant divergence in Millennial value systems manifests in the professional realm. Millennials value freedoms in the workplace more than their predecessors, although Lyons, Duxbury, and Higgins found fewer differences than they expected. Older generations seem to value work for work’s sake, but working conditions and expectations have evolved. American workers today generally spend fewer hours in the office than previous generations, although telecommuting and the widespread expectation of continuous accessibility of employees complicates the accuracy of hours worked. Twenge and Campbell noted that Millennials’ desire for leisure aligns with prior generations in parallel with steady advances in technology and workplace productivity that accompany each generation. The authors also found that Millennials are “actually more satisfied with their jobs and want more job security than older generations” despite stereotypes that suggest Millennials seek meaning in their work and lack organizational loyalty. Millennial career priorities also do not greatly differ from previous generations. Five key elements that Millennials value in the workplace are:

---

19 Ibid.
20 Twenge and Campbell, “Who are the Millennials?,” (2012).
21 Ibid.
An additional and critical element to what Millennials want in the workplace is the “happiness factor.” According to a 2016 study, much of what Millennials desire is shared with previous generations, although Millennials' desire for more work-life balance is particularly pronounced. A study conducted by Fidelity Investments concluded that Millennials aged 25 to 35 would be willing to give up an average of $7,600 in annual pay for greater work-life balance and career development opportunities. Millennials generally prioritize the values of their employer and how they align with their own over their salary. Furthermore, Millennials are overwhelmingly more likely to remain with an employer if that employer values a healthy work-life balance.

A comparison of Millennial workplace desires to those of other generations does not support the stereotypical narrative that Millennials are demanding and entitled. On the contrary, Baby Boomers and Generation X employees provided similar answers to survey questions about workplace environments. All three generations valued a boss they can respect, effective communication, a safe work environment, teamwork, and a diverse workforce. Millennials and their generational predecessors all rated retirement plans, health care, compensation and job security as important workplace benefits. Additionally, all prioritized a workplace that encourages employee input, the provision of good training and skills, merit-based advancement, and promotions from within.

---

22 Brandon Carter, "Millennial Employee Engagement & Loyalty Statistics: The Ultimate Collection," (2018). This particular resource displays up to date information on surveys and other data on millennials and millennials in the workplace. The 5 key elements in this work are representative of some of the main consistencies and conclusions drawn from these data.
26 Ibid.
27 Ibid.
28 Ibid.
Millennials are less concerned about surveillance than older individuals, even within the workplace. In 2015, 54% of individuals surveyed in a Pew Research Center report stated that they would be comfortable with surveillance cameras using facial recognition technology to prevent workplace thefts. An additional 21% said ‘it depends’ and only 24% said that this would be unacceptable. Issues of technology, information security and device security were ranked higher in importance than surveillance across all age groups, with only 38% of individuals listing surveillance in their top three concerns.

Concerns about surveillance are tertiary to information and device security, and Millennial values regarding personal privacy differ from other generations. Even though 57% of younger digital natives are aware that companies buy and sell their personal data, 52% are comfortable sharing their location with smartphone apps for practical purposes (i.e., for navigation). Conversely, only 17% of older generations are comfortable sharing that same personal data, highlighting the significant gap

---

30 Ibid.
between digital natives and their willingness to give up data “when it makes sense to do so.”

Additionally, a Pew Research Center report found that 57% of individuals ages 18-49 think their personal data is either more secure than or just as secure as it was five years ago. On the other hand, only 42% percent of those aged fifty and older believe their data is as secure as it was five years ago. Such statistics indicate that younger individuals are more trusting of data protection practices in place today than previous generations.

Key Finding 2: Public Sector Organizations Can Incorporate Flat Organizational Structures to Promote Millennial Values and Mitigate Insider Threat Risk Factors.

---

While there is a fair amount of documentation and recommendations on implementing the technological solutions to insider threat prevention, there is less guidance on addressing organizational culture as a weapon against insider threat. Certain private-sector organizations can provide this guidance. More specifically, these organizations can provide insight into ways organizations can leverage Millennial culture and values to minimize the risk of insider threat development.

"Rather than expecting [cultural] models from smaller, start-up-style organizations to flourish in large, established bureaucracies, government agencies can examine the models that other large and complex organizations, such as General Electric, Dell, or IBM, create."

Studying Millennial outreach programs of large corporations with entrenched bureaucracies could potentially highlight effective options for combating insider threat through organizational culture. Three salient examples of these best practices from the private sector are: emphasizing career development and mentorship to improve Millennial satisfaction in the workplace, creating a flexible workplace to attract Millennial employees, and fostering a sense of purpose and altruism in corporate culture to inspire Millennial employees.

The U.S. Government’s cultural approaches to insider threat may be different from those of the private sector, especially given structural and legal differences between the two. Rather than expecting models from smaller, start-up-style organizations to flourish in large, established bureaucracies, government agencies can examine the models that other large and complex organizations, such as General Electric, Dell, or IBM, create. The way these private sector giants are adapting to generational cultures and the roadblocks they have run into can be indicative of the best practices to pursue in the change-resistant and resource-limited environments that define many government agencies.

---

34 Karl Wagner interview by authors, February 22, 2018.
35 Ibid.
At many large corporations, the annual review—in which workers sit down with their managers to review their performance—is the standard benchmark from which to judge how employees contributed throughout the year. These same organizations are now finding that Millennials greatly dislike this practice, and instead prefer consistent feedback in the form of “coaching.” Frequent and constructive advice helps Millennials quickly adapt and feel confident in their work. Moreover, giving Millennials a way to request and receive feedback allows them to feel more engaged with the organization and more empowered over the direction of their careers. General Electric, under its previous CEO Jack Welch, had a reputation for implementing a particularly aggressive and rigid annual review structure. Now the company has switched to what it describes as “frequent conversations,” whereby managers and employees discuss feedback on a much more consistent basis, even developing an app to help in the

---

process. Employees can request feedback at any point through their smartphones and there is even an option to direct the request to other senior staff, irrespective of whether the employee reports to them. The goal, according to GE, is not to grade how well people are performing but rather to encourage improvement, a Millennial value that corporations can easily address. Areas primed for improvement, like educational initiatives to distinguish whistleblowing from leaking and effective hierarchy-quashing channels for complaints, also merit inter-disciplinary solutions. In today’s world, hierarchies are becoming increasingly problematic for organizations seeking efficient communication and collaboration. By their very design, hierarchies create separation between employees and the core layers of management (first, middle, and upper). While effective at demarcating levels of authority and establishing clear lines of communication, this model also stagnates change and impedes collaboration. With communication typically flowing from top to bottom, interdepartmental discourse suffers and employee requests must travel through many layers of intermediaries before they can be considered and implemented. In light of these drawbacks, hierarchies must give special consideration to structures that facilitate communication and connection and promote responsiveness—especially as the

![Comparing Traditional & Millennial Organizational Structures](https://bit.ly/2aEtUJS)

42 Ibid.
organization grows and the gap between upper-level managers and employees expands.\textsuperscript{46}

One such structure is a ‘flatter’ organizational design, which seeks to open lines of communication and reduce layers within the organization while maintaining the shape and function of traditional hierarchy. These structures help large, hierarchical organizations create the effect of more intimate or ‘start-up style’ companies by bringing employees and leadership into greater contact through internal messaging platforms or fewer ‘middle managers’ signing-off on decisions and new initiatives.\textsuperscript{47} Not every company can offer the relaxed work environment of Google, and it is both unrealistic and unadvisable for large, established hierarchies to throw out organizational charts and drastically restructure their managerial system. But all hierarchies can adopt minor changes and incorporate new elements of communication and collaboration to gradually shift towards a flatter design. Companies that have done so, such as the energy giant Semco, which has gradually distributed decision-making authority over the last three decades, report enhanced innovation and performance. Though often a tough sell at the outset, shifting towards a flatter structure is both attainable and advisable for organizations seeking a more productive and engaged workplace with improved communication from the bottom-up.\textsuperscript{48}

Flatter structures are also advisable from a security standpoint, as insider threat prevention programs run into structural challenges within highly hierarchical organizations. Hierarchical organizations tend to discourage internal or lawful disclosures by exerting stricter control and a greater fear of retaliation on lower-level employees. Whistleblowing that does occur in hierarchies tends to be centralized at the upper managerial level, wherein leaders have greater discretion and power, and diminished fears of retaliation. As such, insider threat strategies designed to encourage employees to disclose concerns or report suspicious activities can be expected to face increased resistance and diminished returns at the lower levels of large, hierarchical organizations.\textsuperscript{49} Conversely, flatter organizational structures promote internally expressed criticism and lawful disclosures.\textsuperscript{50} With fewer managerial barriers and enhanced collaboration, employees in flatter or more open organizations feel more confident that leaders

will be receptive and responsive to their concerns—a key determinant of whether employees will use internal mechanisms to blow the whistle on wrongdoings.  

Hierarchy isolates vertical levels of management and horizontal departments, impeding action with overlapping or disconnected stages of review and implementation. This siloed organizing principle is particularly problematic for coordination between first-level and upper-level management. First-level managers serve as the front lines of leadership through direct interaction with employees, but often lack allegiance to either their superiors or subordinates. A lack of cross-organizational buy-in and shared priorities necessitates the development of a management corps to integrate messaging, align policies, and process reports between levels and departments.

This is not to say employees in hierarchical organizations will never flag wrongdoings or express grievances. Using internal reporting mechanisms is possible, but doing so involves an intimidating range of psychological and institutional barriers employees must overcome. First, muddled protocols on lawful disclosures, both at the organizational and federal level, often stoke fears of reprisal among lower-level employees. A 2011 U.S. Merit Systems Protection Board study revealed that approximately one-third of federal employees “who felt they had been identified as a source of a report of wrongdoing also perceived either threats or acts of reprisal, or both.” The report cited a disconnect between management protocols and workforce perception of reprisal as the main source of employees’ trepidation. Furthermore, processing reported wrongdoings through a tiered review process often takes weeks or months in large bureaucracies. Fragmented communication between each managerial level and multiple entities

55 Ibid.
56 Ibid.
complicates the connection of concerned employees with a receptive leader, and can deter reporting altogether.\textsuperscript{57} Given these barriers, employees seeking to efficiently or decisively draw attention to a grievance may find that external and unauthorized channels are the more compelling option.\textsuperscript{58}

**Key Finding 3: Fewer Millennials are Attempting to Harm Their Company Than Members of Other Generations.**

Despite an inherent skepticism of Millennials in the workforce, there is currently scant evidence that Millennials pose a more significant threat of becoming insider threats to organizations than previous generations. The CERT Division of the Software Engineering Institute at Carnegie Mellon University houses the National Insider Threat Center (NITC). NITC collects data on insider threat incidents and compiles it in the CERT National Insider Threat Center Incident Corpus.\textsuperscript{59} The dataset is not all-inclusive, but does include those insider threats that companies have made public. The data suggest, however, that Millennials are currently responsible for fewer malicious insider threat incidents than anticipated.\textsuperscript{60} While CERT’s database lists only 98 malicious Millennial insiders, Pew Research Center workforce projects suggested that Millennials could have been responsible for 350 of the 1,029 record insider threat incidents based on their proportion of the workforce. Using the same set of statistics, CERT anticipated that Gen X’ers would be responsible for 350 incidents. In fact, Gen X’ers have perpetrated nearly 400 recorded incidents. This sample suggests that Millennials, unlike other generations, act as intentional insider threats at a lower rate relative to their workforce size.\textsuperscript{61}

\textsuperscript{58} Ursula Oswald Spring et al., “Peace Studies,” (2010).
\textsuperscript{59} Miller, S. (CERT Division of the Software Engineering Institute and Carnegie Mellon University).
\textsuperscript{60} Ibid.
\textsuperscript{61} There are some caveats to these data. First, the data also list 286 incidents in which the perpetrator’s age is unknown or unclear. Second, Millennials only recently became the largest generation in the workforce and the youngest members are just now entering the workforce. One could argue that as a relatively young generation, Millennials simply have not yet had the time to encounter the later life crises that often prompt insider threat development. On a similar note, Millennials are generally underemployed, and therefore, many may not be in positions that make intentional insider threat incidents possible. Last, the data only covers known incidents.
Several factors may be responsible for the disparity between expected and actual levels of Millennial insider threat. First, Millennials report lower rates of job satisfaction compared to their predecessors. A 2016 Gallup report indicates that in the current workforce, Millennials are the generation least engaged - emotionally and behaviorally connected - with their job and organization.\(^62\) Gallup’s findings state that only 29 percent of Millennials consider themselves engaged at work, compared to 32 percent of Generation X and 33 percent of Baby Boomers. Most important, 16 percent of Millennials were “actively disengaged”—seeking to damage their organization and therefore, by definition, acting as insider threats.\(^63\) Despite being the least engaged generation, fewer Millennials are “actively disengaged” than Generation X (18 percent) and Baby Boomers (19 percent).\(^64\) These data suggest that Millennials feel less loyalty to the organization and spend more time participating in unrelated activities while at work, yet are still less likely than their Generation X colleagues to become insider threats.

\(^{63}\) Ibid.
\(^{64}\) Ibid.
In addition to being unengaged at work, research suggests that Millennials are more likely to change jobs than their predecessors. In 2017, Deloitte conducted a survey which indicated that in 2016, 66 percent of Millennials intended to leave their current job within the next two years, while only 27 percent planned to stay for five years or more. These figures changed to 45 percent and 31 percent respectively, suggesting an upward trend toward job longevity. At the same time in the United States, the number of Millennials intending to stay at their current employment for five years or more exceeded the number of those anticipating an imminent departure, though not by much (35 percent and 32 percent, respectively). Depending on interpretation, this data could indicate less loyalty—an insider threat risk—in the Millennial population, or a willingness to change jobs when not satisfied—a positive way to seek better employment rather than stay and harm the company.

The 2017 Deloitte survey also indicated that despite seeking new employment, 70 percent of Millennials from developed economies prefer full-time and permanent positions to short-term, freelance jobs. Deloitte attributed this desire for stability to a lack of Millennial optimism.

---

66 Deloitte conducted this survey among 8,000 Millennials from thirty different countries. These individuals all had college degrees, were employed full-time, and worked in the private sector.
67 Ibid.
68 Ibid.
regarding the economy, thus spurring their search for job security and a fixed income. Without confidence in the economy, Millennials appear to be increasingly risk-averse and are accordingly less willing to seek new employment elsewhere. That many of the survey responses had the qualifier “should the job market improve” supports this theory. Cultural traumas also fuel this insecurity. Millennials began entering the workforce only a few years before the beginning of the Great Recession, and, while in many ways the economy has recovered, Millennial faith in financial institutions and the overall health of the economy has not.

One possible interpretation of the data is that the high turnover rate implies less loyalty among Millennials, potentially spurring insider threat development. Alternatively, the combination of figures regarding job change with the percentage of employee dissatisfaction presents another possibility: rather than stay in an unhappy job, many Millennials just leave the organization, counting for fewer insider threats in this respect. Additional research supports the latter interpretation. Millennials are increasingly reporting that they pursue jobs that allow them

---

70 Ibid.
71 Ibid.
to feel as if they are contributing both to their organization and society as a whole. In 2014, over half of Millennials surveyed reported that an organization’s policies on corporate social responsibility directly impacted their decision to accept an offer from that organization.\textsuperscript{73} Other research suggests that organizations offering employee volunteer opportunities report higher levels of engagement and productivity.\textsuperscript{74} According to the Harvard Business Review, employees who feel inspired, “deriv[ing] meaning and purpose from the company’s mission,” are more than twice as productive as employees who are disengaged.\textsuperscript{75} This social responsibility manifests itself throughout the employment process. The 2016 Deloitte Survey reported that 82 percent of Millennials intending to stay at their organization for at least five years believed that they shared their own values with the organization.\textsuperscript{76} A 2012 survey found that two-thirds of Millennials wanted their employers to be socially engaged compared to only 50 percent of non-Millennials.\textsuperscript{77} These trends suggest that providing Millennials with a clear path to participate in the kind of public good that studies have consistently shown the generation desires is an effective means of increasing their satisfaction with employers and companies, thus potentially reducing the development of insider threats.\textsuperscript{78}

Many prominent organizations have already harnessed Millennial’s desire to give back through their work, with improved outcomes for both the organization and the community. Marriott International instituted a program which incentivizes employees to volunteer one week per year with an organization of their choosing.\textsuperscript{79} Employees receive both their regular compensation and special recognition throughout the organization for their contribution.\textsuperscript{80} The organization and the employees equally feel the benefits of this program. Not only does Marriott receive positive press for giving back to the community, but the program may also encourage increased productivity and satisfaction among its Millennial workforce.\textsuperscript{81} While such a program

\textsuperscript{73} Mei Cobb, “Passion for a Cause: Millennials Want to Work and Volunteer Together,” (2014).
\textsuperscript{74} Stephanie Vozza, “Why Every Company Should Pay Employees to Volunteer,” (2014).
\textsuperscript{75} Eric Garton and Michael Mankins, “Engaging Your Employees Is Good, but Don’t Stop There,” (2015).
\textsuperscript{76} Deloitte, “The 2016 Deloitte Millennial Survey – Winning over the next generation of leaders.”
\textsuperscript{78} Eric Garton and Michael Mankins, “Engaging Your Employees Is Good, but Don’t Stop There,” (2015).
\textsuperscript{79} Marriott News Center “Marriott International Unveils Global Sustainability and Social Impact Commitments to Deliver Positive Change,” (2017).
\textsuperscript{80} Ibid.
\textsuperscript{81} Lauren Vesty, “Millennial (2016)s.”
alone will neither transform organizational culture nor eradicate insider threat, it could satisfy the need for a sense of purpose that Millennials report desiring in their careers and instill pride towards their employers, making insider threats less likely.

In addition, although idealism drives Millennials, financial security is still a primary concern. The current economic situation for Millennials is far from perfect. As explained earlier, advanced employment prospects are dim, wages have stagnated, living costs have risen, and the amount of student loan debt continues to increase. Tuition costs alone have increased over 500 percent since 1978. Most Millennials believe that finding a full-time, well-paying job is harder for them than it was for earlier generations. Members of the older generations overwhelmingly agree with this conclusion. For Millennials, financial instability means that money is still a significant motivating factor in determining whether to stay with an organization. As salaries often increase when transferring to a new job, the apparent Millennial tendency to job-hop is not surprising. One study found that half of Millennials stated that they would consider another job for a raise of 20 percent or less. Many Millennials are confident that they will eventually earn enough money to enjoy the lifestyle they want, but they must ‘get there’ first. In the meantime, they need to make enough money to cope with their various financial obligations. An opportunity at a different organization that offers a higher paycheck is understandably enticing. Those who complain of Millennial greed and job-hopping are confusing disloyalty with pragmatism. Assisting with this financial burden could not only promote employee engagement and loyalty, but actively combat a potential motivation for committing insider threat incidents.

Key Finding 4: Millennials’ Workplace Preferences and Device Usage Pose Challenges for Insider Threat Prevention and Detection.

Given the rapid change in technology and communications over the last two decades, Millennial work preferences have become increasingly incompatible with the structure and

---

83 David Barnes et al., 2016 State of the Millennial Report: A Review of the Challenges and Opportunities for Young Americans (2016).
84 Ronald Brownstein, “Even Baby Boomers Think It’s Harder to Get Started Than It Used to Be,” (2015).
function of most large organizations.\textsuperscript{87} The Deloitte 2016 Millennial Survey revealed that 88 percent of Millennials surveyed wished they had more say as to when their work day starts and ends. A further 75 percent wanted to have the ability to work remotely. As of today, only 43 percent of Millennials have either opportunity.\textsuperscript{88} This is an oft-cited reason for why Millennials are dissatisfied at work, and may contribute to why 66 percent of the generation reported that they planned to leave their current organization within the next three years.\textsuperscript{89}

Evidence shows that embracing a flexible work system not only helps with employee morale, but also has no ill-effect on overall productivity. Millennials often attribute low workplace satisfaction to long commutes resulting from a lack of dependable public transportation, high living costs near urban offices, and anachronistic requirements for employees to report work at the same time and location every day. More flexible work environments can circumvent many of these stressors, potentially mitigating resentments that could ultimately fester into insider threats.\textsuperscript{90} The core requirements to launch such a program are minimal: a flexible work environment can mean less capital investment for companies, such as providing access to laptops with virtual private networks (VPNs) rather than larger hardware systems. Beyond investment concerns, flexible work entails implementing clearly delineated parameters as to which roles may or may not work remotely.\textsuperscript{91}

Some large organizations are changing their expectations of the workday in order to respond to the desire for greater work flexibility. Dell, for example, has taken the lead in pushing a non-traditional workday and experienced no loss in productivity.\textsuperscript{92} With a workforce that already works from home 25 percent of the time, and an aim to increase that number to 50 percent by 2020, Dell employees have freedom to decide where they work--excluding those who

\textsuperscript{88} Ibid.
\textsuperscript{89} Ibid.
\textsuperscript{90} Ibid.
\textsuperscript{92} Jeanne Sahadi, “Dell Really Wants You to Work from Home ... If You Want,” (2016).
are involved in the physical manufacturing side of the business.\textsuperscript{93} Furthermore, Dell employees have the autonomy to decide when their work day begins and ends once they have manager approval for a flex schedule.\textsuperscript{94} Because employees are only coming in a few times a week, the company has saved $12 million a year by consolidating its physical office space. Dell’s efforts have created a more open and flexible environment more attractive to Millennials and reportedly has not led to a loss in creativity.\textsuperscript{95} The shift is a promising example of how workplace norms that are not typically associated with insider threat can change in small ways that empower a large portion of a company’s workforce.

Mobile devices have made working outside a traditional office much easier for employees. Many Americans already own a smartphone and a laptop, thereby permitting employees to use their personal devices for work purposes rather than company-owned devices. This policy is also more cost-effective, as organizations save an average of $350 per year for each employee not issued a company device.\textsuperscript{96} Because of these incentives, 87 percent of organizations now depend on their employees to use their personal devices for some work purposes.\textsuperscript{97} As digital natives, Millennial employees are likely to see these as positive workplace developments.

Yet there are risks associated with a more flexible work environment. Allowing employees to use their personal devices for work may leave an organization’s data vulnerable to hacking, theft, or intentional leaks. If an organization does not issue devices to its employees, it is more difficult to ensure consistent security with the myriad of devices that employees use in their personal lives. Instances of malware have been on the rise, especially on the Android operating system; security researchers found that almost 90 percent of Android devices are exposed to at least one critical vulnerability, and malware developers have created evasion techniques to circumvent commonly used security products.\textsuperscript{98} \textsuperscript{99} Malware can enable attackers to steal usernames and passwords, spy on the user’s activities or access data on the phone, serving as a backdoor entry into an organization’s systems.

\textsuperscript{93} Ibid.
\textsuperscript{94} Ibid.
\textsuperscript{95} Ibid.
Employees may also be less concerned about security risks on their personal devices than they would be if they were using a company-issued device. While Millennials are known for being tech-savvy, this does not translate into a heightened awareness of cyber security risks. Pew Research Center data show that across a variety of social media and internet applications, people aged eighteen to twenty-nine are consistently the earliest adopters of new apps and comprise the highest percent of users.\textsuperscript{100} Millennials often pay little attention to the potential security vulnerabilities that new technologies and devices pose, or the risks associated with downloading certain apps or connecting to a public Wifi network without a VPN.\textsuperscript{101}

The proliferation of unsecured devices exposes Millennials and other digital natives to greater insider threat vulnerabilities. As ownership of technical devices grows, Millennials frequently represent the most saturated market demographic, with 94 percent of the 18-29 age bracket possessing a smartphone.\textsuperscript{102} Well-accustomed to this technology, Millennials routinely click through lengthy user agreements without reading the terms and conditions, thereby ceding control for convenience on a daily basis.\textsuperscript{103} The unprecedented number of personal devices running various unknown applications significantly increases the likelihood that employees with access to a company’s network will inadvertently facilitate an external attack. For instance, Symantec observed 13.6 million malware attacks against mobile devices in 2016, a 105% increase from 2015.\textsuperscript{104}

\textsuperscript{100} Pew Research Center, “Social Media Fact Sheet: Demographics of Social Media Users and Adoption in the United States,” (2018).
\textsuperscript{101} Pew Research Center, “Social Media Fact Sheet.”
\textsuperscript{102} Ibid.
Social media usage in the United States has become ubiquitous, with 69 percent of adults owning at least one online account as of January 2018 and nearly 75 percent of Facebook users visiting the site every day. Social media accounts present opportunities for employees to either knowingly or inadvertently compromise an organization’s assets. The amount of personal and professional information that can be found by analyzing an individual’s online profiles makes it possible for malicious actors to conduct social engineering and use someone’s information against them. Attackers can use LinkedIn connections and profile data to create a map of an organization’s workforce and determine who has access to important information, or scrutinize Facebook profiles for hints of unhappiness in the lives of employees. Armed with this information, the attacker could contact an employee directly and attempt to gain desired information. Or, the attacker could use the personal information gleaned from social media to create a convincing spear phishing email that might grant them an entry into the organization’s systems—a tactic that 67 percent of cybersecurity experts consider to be the biggest vulnerability for unintentional insider threats. It is also possible for an attacker to use the information from social media to compromise a user’s email or computer login credentials by resetting the password or utilizing other threat vectors. These issues are not exclusive to millennials; unhygienic technology practices and the proliferation of personal information online affects all demographics and all organizations. However, the percentage of Millennials that own and actively use personal devices means that vulnerabilities to hacking and targeting are particularly high, especially considering the fact that Millennials recently surpassed all other generations as a percentage of the workforce.
Key Finding 5: Technology Dependency May Reduce Millennials’ Ability to Cope with Professional Stressors and Personal Crises

Unparalleled advances in digital technology are redefining how Millennials think, behave and interact with others in both the workplace and online. The rapid spread and transformation of digital technology began in the early 1980’s and has accelerated ever since, creating a generational divide between “digital natives” who were born after 1980 and grew up speaking the digital language of computers, video games and the Internet, and “digital immigrants” who were not born into the digital world. Being a digital native constitutes a core component of the Millennial identity. Constant interaction with communications technology and digital environments has not only influenced Millennials’ work habits and preferences, but has also caused this generation to “think and process information fundamentally differently from their predecessors,” according to education researcher Marc Prensky.105 These changes create both opportunities and vulnerabilities for organizations attempting to assimilate this first generation of digital natives into the workforce. In particular, the impact of technology on three key psychological conditions--personality vulnerabilities, maladaptive coping mechanisms and susceptibility to online targeting--could influence how organizations approach the challenge of preventing insider threat among Millennials and future generations of digital natives.

Personality dysfunction is one of the key factors that predisposes individuals of any generation to commit insider threat.106 When asked to form a personality archetype of an insider threat, twenty senior intelligence community professionals identified psychopathy, malignant narcissism, and borderline personality organization as the most prevalent traits.107 The 2005 Krofcheck and Gelles Training and Reference Manual for Personnel Security Professionals similarly highlighted individuals with antisocial and narcissistic personality disorders as the greatest security risks.108 Counterintelligence psychologists also include immaturity—the

108 Ibid.
inability to control emotional impulse, moderate behavior to social norms, and separate fact from fiction—and ethical flexibility as underlying attributes of these disorders.\(^{109}\)

Continuous exposure to networked technologies such as the Internet, social media, and mobile phones—a symptom of the digital native—can create a technology dependency that reinforces the personality disorders and vulnerabilities associated with insider threat.\(^{110}\) Social media platforms, for example, can serve as an instrument for self-promotion and exhibitionism, leading multiple studies to link social media use with a growing culture of self-centeredness. An analysis of narcissism and empathy levels among college students over the last thirty years found that narcissism has increased while empathy has decreased exponentially since 2000.\(^{111}\) Internet addiction, which follows the same neurobiological cycle as other chemical addictions, may also amplify personality dysfunctions among digital natives.\(^{112}\) The Internet provides the user with a dopaminergic release, thereby creating a positive reward during use and a reward-deficiency that prompts withdrawal-like symptoms when not in use. Over time, the user develops a tolerance to the positive effect and requires more use to generate the same level of satisfaction. As a result, the Internet increasingly becomes a tool for mood modification in coping with, or escaping from, the various stresses of life. This compulsive use often impedes personal and professional function and increases anxiety, depression, irritability, and lack of emotional control.\(^{113}\) Combined with other risk factors such as financial security or personal crisis, technology dependency could further predispose individuals with dysfunctional personality traits to commit insider attacks. As more and more of the workforce become digital natives, an insider threat program should be aware of these vulnerabilities.

In addition to personality disorders, insider threat literature indicates that chronic personal or professional life stressors are consistently the driving forces that impair cognitive functioning and judgment and eventually push a disgruntled individual to act out against their


\(^{111}\) Elliot T. Panek, Yioryos Nardis, and Sara Konrath, “Mirror or Megaphone?: How relationships between narcissism and social networking sit use differ on Facebook and Twitter,” (2013).

\(^{112}\) Ibid.

organization. Interpersonal relationships and a sense of belonging at work, however, can help employees cope with stressful personal events that often precipitate insider threat. When a crisis intensifies and impairs rational judgment, strong relationships often restrain an individual from undertaking impulsive actions, including insider attacks, to relieve the mounting pressure.

Millennials’ tendency to use the virtual world to fulfill social needs may reduce the benefits gained from interpersonal relationships and subsequently undercut their ability to cope with critical life stressors. Strong interpersonal relationships, whether between individuals or an employee and their organization, require a great deal of time, energy, and social interaction to maintain. Cyber relationships based in social media are comparatively transient and easy to maintain on a superficial level. Text and digital communication reduce the anxiety felt in face-to-face interactions, which in turn can diminish Millennials’ ability to cope with the effects of rejection or disapproval. Despite the ability to continuously connect with friends, higher levels of social media use are counterintuitively associated with higher perceived social isolation (PSI). In a study evaluating the social media habits of US adults aged nineteen through thirty-two, those in the top 25 percent of time spent on social media had twice the odds of possessing a higher PSI than those in the lowest 25 percent. One explanation for this association is that social media presents routine evidence of social exclusion and promotes social comparisons between oneself and a highly curated portrayal of others. This comparison encourages the belief that others are happier, more successful, and more connected, thereby intensifying personal feelings of loneliness and depression.

Living in the virtual realm creates further insider threat risks in the form of online targeting. Social psychologists have shown that the characteristics of open forums—anonymity, sensory overload, and loss of responsibility—can reduce self-awareness and promote uninhibited

---

115 Ibid.
117 Donna J. Reid and Fraser Reid, “Text or Talk? Social Anxiety, Loneliness, and Divergent Preferences for Cell Phone Use,” (2007).
118 Brian A. Primack et al., "Social Media Use and Perceived Social Isolation Among Young Adults in the U.S." (2017).
behavior that social evaluation typically restraints.\textsuperscript{119} Search engines make the Internet an especially dangerous place for emotionally compromised individuals because they are empowered to self-select which content and conversations to engage.\textsuperscript{120} Even on social media, individuals tend to remove dissonance by self-segregating to produce an experience more in line with his or her personal views.\textsuperscript{121} An individual online is therefore more likely to seek out reinforcement for his or her disgruntlement than potentially unpleasant, but accurate, advice from a friend.\textsuperscript{122} These outlets can take the form of message boards on Reddit or Facebook, or worse, unauthorized disclosure sites such as Wikileaks. Moreover, the anonymity of the Internet increases the ease with which a malicious actor can target an online user displaying career disgruntlement or personal vulnerabilities and manipulate him or her into committing insider threat.\textsuperscript{123} Taken together, these technology-induced behaviors can undercut community engagement and diminish interpersonal relationships among digital natives. Not only does disconnection this impact personal and workplace satisfaction, but also limits the number of individuals and groups who might detect life crises and provide critical emotional support--thereby removing a critical barrier preventing insider threat.\textsuperscript{124}

\textsuperscript{120} Elanor Colleoni, Alessandro Rossa, and Adam Arvidsson, “Echo Chamber or Public Sphere? Predicting Political Orientation and Measuring Political Homophily in Twitter Using Big Data,” (2014).
\textsuperscript{121} Ibid.
\textsuperscript{122} Ibid.
\textsuperscript{124} Primack et al. “Social Media Use,” (2017).
VII. RECOMMENDATIONS

Recommendation 1: Private and Public Organizations Should Reinstate Programs that Reward Employee Longevity and Provide Pathways for Professional Development.

"Millennials suffer from stagnant wages, an increased cost of living, and significant student loan debt. At the same time, many organizations have drastically reduced or ended traditional employee benefit programs."

The ever-worsening financial situations of Millennials entering the workforce creates significant vulnerabilities. Millennials entered the workforce under the shadow of the Great Recession and their professional experience has been largely negative. At the same time, many organizations have slashed or ended traditional employee benefit programs. In this perfect storm, Millennials have less opportunity to retire with a pension than previous generations. These risks to employees translate into potential insider threat risks for employers.

Organizations wishing to avert the risk of insider threats among Millennial employees should reinstate programs that reward employee longevity and advancement within an organization. One way to offer this reward is to institute programs to help Millennials cope with their current financial burden. Competitive salaries and assistive programs could generate stability and cultivate organizational loyalty by increasing the time and emotional investment placed in an organization, thereby lowering the risk of insider threat development. The US government, for example, offers student loan forgiveness in exchange for ten years of public service. Some private sector organizations are developing similar programs. According to survey research by

---

125 Mark Kelton interview by authors, January 29, 2018.
128 Ibid.
130 Jessica Mai, “7 companies that help employees pay off student loan debt,” (2016).
Deloitte, Millennials desire economic stability and do not change jobs because of ambivalence or disloyalty.\textsuperscript{131} While recognizing that the primary mission of most private sector companies is to make a profit, employee disengagement hampers productivity and the high turnover rates among Millennials are causing significant financial losses.\textsuperscript{132} If implemented, this recommendation could both boost productivity and promote employee loyalty.

**Recommendation 2: Organizations Should Prioritize Employee Community-Building Events that Increase Face-to-Face Interaction.**

To help employees feel connected with their colleagues and to promote feelings of good will, organizations should encourage group events among their workforce. The increased connectivity that technology provides creates a sense of urgency that can disrupt a healthy work-life balance, and can lead to feelings of isolation. By contrast, face-to-face, rather than virtual, meetings and offline team engagement can build a sense of belonging and community.\textsuperscript{133} Such activities have the potential to break anti-social coping mechanisms and reduce the “holding power” of technology. These activities can also ground the individual with intimate interpersonal relationships that improve organizational loyalty and provide outlets to constructively deal with negative life events.\textsuperscript{134} Organizations can promote mutually invested goals (i.e., fitness) to improve work-life balance, increase positive health outcomes, and build a sense of community.\textsuperscript{135} Since many health insurance providers offer premium deductions to incentivize behavior that decreases susceptibility to chronic health conditions, organizational fitness programs could increase face-to-face interaction and also provide partial relief of Millennials’ financial burdens.

Offering volunteer opportunities and improving corporate social responsibility could also help improve work-life balance and build employee engagement.\textsuperscript{136} Organizations that offer volunteer opportunities and are involved with social causes reported higher levels of employee

\textsuperscript{133} Willyerd, “Millennials Want to Be Coached at Work,” (2015).
\textsuperscript{134} Stephanie Vozza, “Why Every Company Should Pay Employees to Volunteer,” (2014).
\textsuperscript{135} Lily Dayton, “Designing a workplace to keep millennials healthy and happy,” (2016).
\textsuperscript{136} Ibid.
engagement and retention.\textsuperscript{137} Such actions offer new employees a sense of fulfillment by increasing the sentiment that they are making a meaningful contribution to their organization’s reputation and society, thereby fostering their likelihood to remain at that organization.\textsuperscript{138} Organizations could also encourage meaningful employee engagement through intergenerational mentorship programs based on the mutual exchange of professional lessons and personal experiences. Such programs would generate a better mutual understanding between generations, as well as develop leadership skills in senior employees and professional education for more junior employees.\textsuperscript{139} Mentorship programs would have the added benefit of building strong professional connections that could create greater workplace engagement and increase awareness of new job opportunities through networking.\textsuperscript{140}

\begin{flushright}
\textsuperscript{137} Ibid. \\
\textsuperscript{138} Garton and Mankins, “Engaging Your Employees Is Good, but Don’t Stop There,” (2015). \\
\textsuperscript{139} Jeanne C. Meister and Karie Willyerd, “Mentoring Millennials,” (2010). \\
\textsuperscript{140} Ibid.
\end{flushright}

Organizations that incorporate elements of ‘flatter’ organizations can ease the rigid hierarchy prevalent among large bureaucracies and promote innovation and collaboration, thereby increasing communication and reducing the risk of an employee becoming an insider threat.141 Flatter organizations share common ingredients that enable hierarchical structures to function more like their de-bureaucratized counterparts, without necessitating disruptive systemic change.142 These elements center around enhanced flexibility through mobile workstations, using personal devices, and alternative work schedules.

"One way that organizations can cater to these workplace desires is by moving away from annual reviews and implementing a system that emphasizes frequent feedback and mentoring."

ideological values when crafting a workplace culture, as well as by exposing young graduates and new hires to upper-level managers with highly developed skills and business ethics.143 The US Department of Transportation’s Idea Hub is another example of an internal online community that promotes and enables this type of community-driven ideation. Since its launch in 2010, employees have submitted over 9,000 ideas, with 25,000 comments and 90,000 ratings—a resounding success for an agency innovation prototype.144

Organizations can also alleviate entrenched hierarchies by establishing mechanisms of dialogue between the chain of command and employees to test and maintain the organizational culture. Research indicates that millennials appreciate both honesty and loyalty from their employers, and continuous dialogue will help leaders decide when and where to implement

---

144 Visit https://cms.dot.gov/transition/ideahub to learn more.
changes in innovative and transparent ways for the benefit of current and future employees.\textsuperscript{145} One way that organizations can acknowledge these workplace desires is by moving away from annual reviews and implementing a system that emphasizes continuous feedback and mentoring. Assigning employees a numerical rating system for their performance and offering reviews on an annual basis has proven to be a morale drain for workers, which in turn could promote insider threat development.\textsuperscript{146} By embracing a system of frequent feedback and constructive communication, organizations could create more value in their Millennial workforce. Rather than receiving one-time negative feedback that may impact workers’ career opportunities and salary promotion, mechanisms for continuous feedback and mentoring gives workers a better understanding of their employer’s expectations and encourages worker productivity. Possible applications would include methods to request and receive feedback in a more informal manner, such as email, as well as scheduled, frequent check-ins with managers. Measures such as these can help increase Millennial employee loyalty to the organization. The increased interaction and communication also provides managers with more opportunities to notice an at-risk employee and intervene before that employee becomes an insider threat.

**Recommendation 4: Organizations Should Mitigate the Risk of Insider Threat By Implementing a Comprehensive Structure of Policies and Procedures.**

It is crucial for all organizations to have a comprehensive set of policies and procedures to mitigate insider threat. These measures must include employee education, analysis, an explicit technology use policy, consistent enforcement, and monitoring that incorporates technical and human sensors.\textsuperscript{147} CERT Insider Threat Center’s “Common Sense Guide to Mitigating Insider Threats” also recommends that organizations “monitor and control remote access from all endpoints, including mobile devices.”\textsuperscript{148} Therefore, an organization’s policies and procedures should include the identification of consumer devices that may be brought into the workplace, monitoring for usage of banned devices in the workplace, and a transparent and consistent


\textsuperscript{147} Warren Holt, CISSP, interview by authors, February 15, 2018.

response policy when violations occur. Organizations could strengthen their insider threat policy and procedure structure by including the following components. Any initiatives taken must be legal and adhere to privacy regulations.

Conduct onboarding training focused on social media use

Few people are aware of the threat of social engineering unless they have personally experienced it. Because of this lack of awareness, organizations should train employees during onboarding to make their personal social media profiles less susceptible to social engineering. This may involve helping workers tighten their privacy settings or include specific company policies on what work-related information employees may share online. A compelling way for an organization to demonstrate the danger of social engineering would be to include an onboarding presentation that compiles data from a fictitious employee’s online accounts and demonstrates various ways a malicious actor could use this information to elicit further information from the employee, knowingly or unknowingly.

Hire Device Threat Analysts specifically tasked with analyzing emerging technology and its potential threat to the workplace

With a rapidly evolving technology landscape, organizations should have a team of individuals whose sole focus is to assess security vulnerabilities posed by new devices and emerging technology applications. This team should have a direct and symbiotic relationship with organizational leadership so that once the team identifies a threat, leadership can quickly update their technology-use policies and inform appropriate divisions, such as human resources. Having a team dedicated to identifying emerging security vulnerabilities in consumer electronic devices can limit the extent to which Millennials’ rapid adoption of new technology can cause damage in the workplace. For example, in November 2017, it was discovered that members of the U.S. military overseas had been using the Strava fitness app during jogging, fitness routines, and even patrol routes. This activity, as seen from the Strava heatmap, helped identify U.S. military bases, the locations of which were supposed to be unknown. If there had been careful analysis of wearable fitness devices and their ability to transmit location data, a decision could

have been made to ban the usage of such devices by personnel, and this entire situation might have been avoided.

In order for Device Threat Analysts to be successful, they must be intimately aware of how each piece of company technology works independently and how it interacts with other components. These components can include computer networks, software, hardware, programming, bugs, malware, forensics, and more. The analysis team also needs to monitor technology-focused websites and publications such as KrebsonSecurity, Schneier on Security, Wired, Dark Reading, Security Week, and CSO to stay informed on software, hardware, and device vulnerabilities, as well as upcoming products. Finally, before a new technology or device is permitted for use in the workplace, including personal employee devices, Device Threat Analysts need to acquire and inspect the technology, read its manual, and test for any potential security threats. Of course, employing Device Threat Analysts may require reallocation of funding and resources, the quantities of which will vary depending on an organization’s size and budget. Accordingly, organizations of all sizes should conduct a self-assessment and determine the appropriate amount of resources to be allocated toward employing Device Threat Analysts.

**Implement explicit policies governing the use of electronic devices for remote work**

A comprehensive policy and procedure structure should specify which devices employees can use to complete assignments outside of the workplace and how employees may safely use those devices. If an employee connects to public WiFi at a coffee shop to access work documents, the device could become infected with malware and give bad actors an entry to the company’s internal network.\(^{150}\) To help mitigate this, organizations should issue devices to employees whenever possible and include a VPN and malware software. This will ensure that all devices accessing sensitive information are subject to uniform and stringent controls. Organizations should implement additional measures on these devices to enhance security, such as a feature that prevents the device from connecting to unsecured WiFi networks. Purchasing devices and issuing them to employees may not be feasible for all organizations, especially if the organization does not expect an employee to do a large amount of remote work. In these cases,

---

organizations should take several measures to ensure that employee’s personal devices are as secure as organization-owned devices. Organizations should:

- Install malware protection software on all devices, including smartphones
- Ban personal devices from connecting to unsecured WiFi networks while attempting to access an organization’s data or provide a VPN
- Limit remote access to an organization’s most critical data and require two-step authentication before granting remote access to an organization’s network.

Such measures may not completely remove the risks of allowing personal devices to access an organization’s data, but they will reduce the likelihood of loyal employees becoming unintentional insider threats.

*Include monitoring that integrates technical and human sensors.*

One of the most useful insider threat technology solutions currently available is security information and event management (SIEM) systems, which act as a central hub for data from a variety of sources. A SIEM system will pull information from all of an organization’s insider threat tools and generate alerts when the system detects anomalies.\(^{151}\) Currently, SIEM systems primarily focus on providing an overview of an organization’s technical infrastructure. This focus is important, as many insider threats involve the exfiltration of data. However, there is other information that should be included to reduce false positives—which account for 52 percent of alerts—and give organizations a clearer picture of potential risks from within.\(^{152}\) SIEM systems that integrate multiple vectors of information will provide context to the technical data and allow insider threat prevention programs to operate more efficiently by reducing the drain on resources caused by false positives.

One potential tool for establishing a baseline of an employee’s normal activity is user behavior analytics. Although there are many behavior analytics tools, such as the robust monitoring of employees online behavior both at work and not, privacy concerns make these invasive methods difficult to recommend. A step in between could be an online portal that enables coworkers to submit reports to the insider threat team if certain behaviors in the office concern the employee. Combined with the data from traditional insider threat software solutions,


this information will give security officers a holistic view of each employee and help them determine when someone is in distress or exhibits signs of disengagement with their job. If security officers are able to flag issues with an employee, the organization can take steps to intervene and provide any assistance that may help get them back on track.\textsuperscript{153} This system should focus mainly on assisting employees through difficult periods in their lives and ensuring they are provided with support to remain engaged at work.

**Recommendation 5: The U.S. Government Should Support Educational Programs that Promote Positive Relationships with Technology and Other Generations.**

Insider threat research demonstrates the potential dangers of social media and online behavior. Therefore, the task force recommends educational programs and curricula that teach cyber ethics to forthcoming generations. Growing up and socializing in a cyber environment increases the likelihood that Millennials and future generations will carry the ethical flexibility and immature behavior rewarded online into offline encounters. State and local officials can counter this outcome by enacting broad educational programs in elementary and middle schools to teach youth about the dangers associated with poor online behavior. Millennials currently entering the workforce are more aware than their elders of the expansive possibilities that technology offers.\textsuperscript{154} They may therefore be the best suited to instill cyber ethics into younger generations and act as authority figures to guide youths’ online and offline maturation.\textsuperscript{155}

Despite constituting the largest proportion of the US working population, negative stereotypes about Millennials’ work ethic and value systems abound. Therefore, the Task Force recommends educational campaign that highlights Millennial contributions to the workforce. Finding shared characteristics could alter the prevailing perceptions of Millennials and facilitate a better intergenerational understanding within an age-diverse workforce.

A public outreach campaign, led by the US Department of Labor, that highlights Millennial contributions to the workforce could begin to alter the prevailing stigma associated with Millennials. Despite constituting the largest proportion of the US working population,

negative stereotypes about Millennials’ work ethic and value systems abound.\textsuperscript{156} Much of the current literature on Millennials is negative, as it is written from the perspective of older generations, skewing the narrative and fostering false stereotypes. Millennials often adopt negative impressions about themselves as a result.\textsuperscript{157} Finding shared characteristics could alter the prevailing perceptions of Millennials and facilitate a better intergenerational understanding within an age-diverse workforce. An age bias is prominent within organizations because the professionals with the most experience—older generations—traditionally hold senior positions. Hiring directors who either share the same age or take their direction from organizational leadership often reflect this bias. A public awareness campaign could counter this effect by highlighting the positive attributes of each generation and the ways in which organizations can benefit from integrating each generation’s unique strengths and perspectives.

One of the primary research endeavors of the National Security Critical Issues Task Force (NSCITF) was to investigate how generational differences might influence the perpetrators and victims of insider threat – an issue that spans both the public and private sectors. The team, comprised of Millennials, believed that focusing on their generation--which encompasses the majority of today’s current workforce--might offer unique insights for organizations looking to mitigate insider threat as part of their larger enterprise risk. The first, and arguably most central aspect of the task force’s key findings, was discovering that when it came to value systems and what motivates insider threat actors, Millennials had more in common with their predecessors than not.

Rather than obstruct the discussion that generational discrepancies might provide additional information on insider threat, these commonalities between generations gave NSCITF a baseline to further investigate the numerous variables that might be indicative as to whether or not someone is more likely to commit insider threat, again, with an emphasis on the Millennial generation. The task force found greater variability in Millennials’ preferences concerning their organizational (work) preferences, technology usage, and overall professional engagement. This inconsistency from previous generations provided a lens for the task force in generating its five key findings.

While adapting organizational structures to accommodate generational preferences might lessen the likelihood of an individual to commit insider threat – save for those insider threat perpetrators with pre-disposed pathologies such as psychopathy – one variable the task force found more complex was technology. While the use of technology is a necessity in conducting business operations, each device within a network creates some degree of vulnerability to that system. Any organization seeking to use technology to accommodate organizational structures that align with Millennial’s preferences (such as remote work policies – to name a singular example) must be highly scrutinized to ensure this risk mitigation tactic does not, in fact, create another risk or vulnerability vector. Beyond inherent technological vulnerabilities, technology also fundamentally changes the way digital natives think and interact as alluded to in Key Finding 5. Organizations will have to delicately balance their considerations on how technology
impacts their mission but also their employees on an individual level.

The National Security Critical Issues Task Force’s recommendations largely focus on the prevention of insider threat as well as detection mechanisms such as SIEM solutions as mentioned in Recommendation 4. Equally important, though not a consideration of this study, is how organizations can respond to insider threat once a threat has been detected – something that must be considered when developing insider threat policies and procedures as referenced in Recommendation 4. Moving forward, NSCITF urges organizations to account for the minutiae of generational considerations which may ultimately help their organizations mitigate the pernicious impacts of insider threat.
IX. BIBLIOGRAPHY


Coyne, Michael, interview by authors, January 29, 2018.


Federal Reserve Bank of New York data for Figure 7.


FireEye. “The Numbers Game: How Many Alerts is too Many to Handle?” 2015. https://www2.fiereye.com/rs/848-DID-242/images/rpt-the-numbers-game.pdf?mkt_tok=eyJpIjoiWlRGak5gWXhPRREV4T1ROayIsInQiOiI5cFhFbh6hGRLYTFobmJVbVByY3FxK2UrODJmRmtMc2ZhaGhWWRud1K054NSltKxkRtdk5zVU1KQkNMZURYxURSOUExRGVWdXUwZmdzR2dCYko3Sk14QitPZnppZ2lzeFZYVpxNx5LRIB2NzhrRjNJa21vY01oY1dFbHdlZ0lDQuJ9.


US Bureau of Labor data for Figure 7.

US Census Bureau data for Figure 1.


Wagner, Karl, interview by authors, February 22, 2018.


