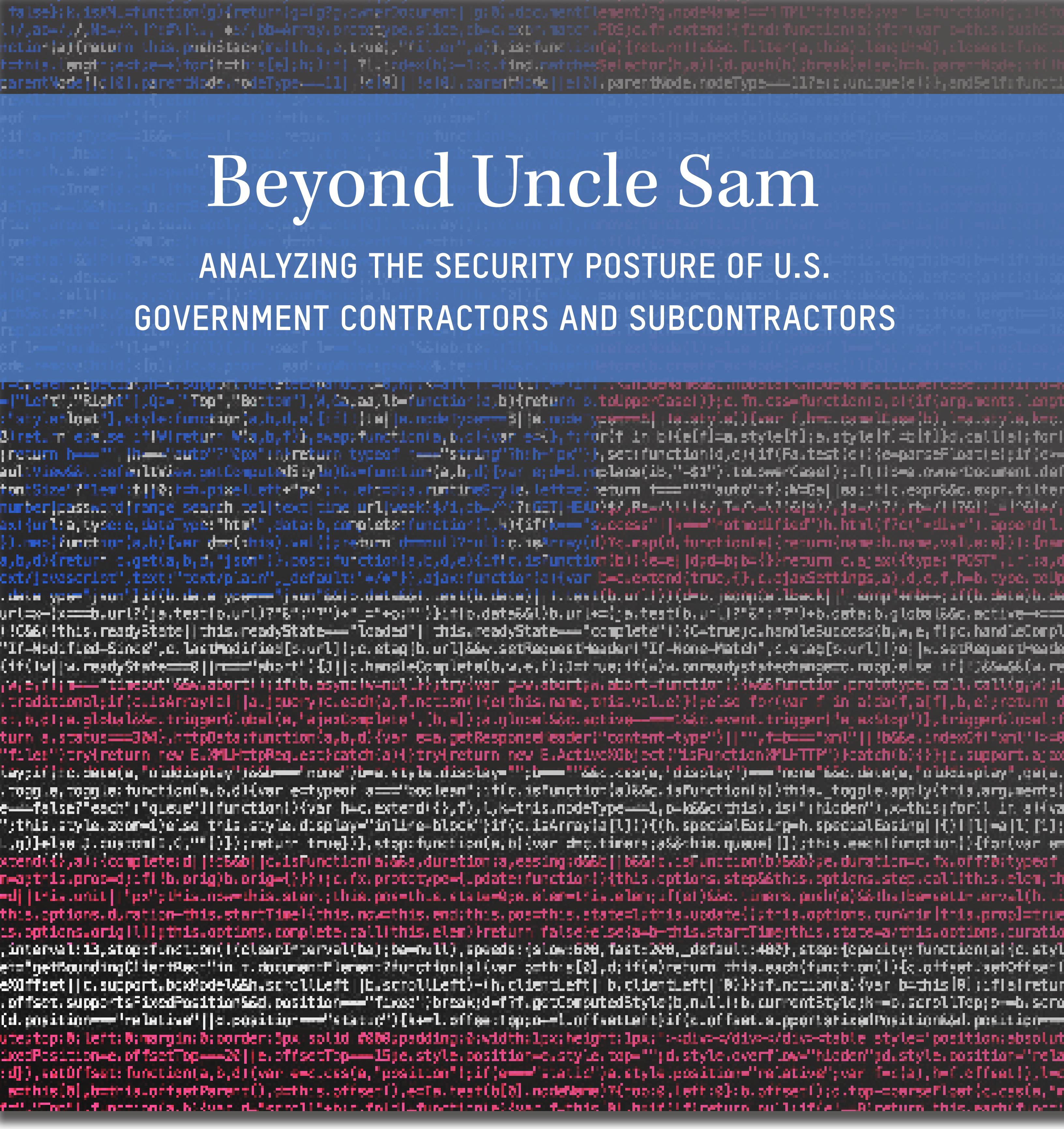


Beyond Uncle Sam

ANALYZING THE SECURITY POSTURE OF U.S. GOVERNMENT CONTRACTORS AND SUBCONTRACTORS

BITSIGHT®
The Standard in SECURITY RATINGS

INTRODUCTION

Understanding and managing cyber risk to the U.S. federal government contractor base has never been more critical. The federal government relies on tens of thousands of contractors and subcontractors -- sometimes referred to as the federal "supply chain" -- to provide critical services, hold or maintain sensitive data, deliver technology, and perform key functions.[1] These organizations are increasingly under cyber attack.

A growing list of contractors and subcontractors have disclosed that they have been victims of data breaches resulting in the compromise of sensitive government information. In response, U.S. federal agencies have or are considering expanding cybersecurity requirements for their contractor base and adopting best practices for evaluating and monitoring those entities.[2]

In a recent study, BitSight found a large gap in the security posture between financial organizations and their third parties.[3] This BitSight Insights report explores a similar question: what is the cybersecurity performance of U.S. federal contractors, and how does that compare to the performance of U.S. federal agencies?

To perform this assessment, BitSight researchers took a random sample of over 1,200 U.S. federal government contractors across the following industries: Aerospace/Defense, Business Services, Healthcare/Wellness, Engineering, Technology, and Manufacturing. The cybersecurity performance of these contractors was compared with the performance of over 120 U.S. federal agencies.

KEY FINDINGS

1. A security performance gap exists between U.S. federal government and its contractor base: **the mean BitSight Security Rating for federal agencies was at least 15 or more points higher than the mean of any contractor sector**.

2. **Over 8% of Healthcare/Wellness contractors have disclosed a data breach since January 2016**; Aerospace/Defense firms had the next highest breach disclosure rate at 5.6%.

3. While the U.S. federal government has made a concerted effort to fight botnets in recent months, **botnet infections are prevalent amongst the government contractor base**, particularly for Healthcare/Wellness and Manufacturing contractors.

4. Many contractors are not following best practices for network encryption and email security: **nearly 50% of contractors have a BitSight grade below C for the Protective Technology subcategory of the NIST Cybersecurity Framework**.

5. **Nearly one in five users at Technology and Aerospace/Defense contractors have an outdated internet browser**, making these employees and their organizations highly susceptible to new variants of malware.

COMPARISON OF SECURITY POSTURE

There is a significant gap between the security performance of U.S. federal agencies and their contractors. To some this may be surprising: some agencies have made public their large data breaches in recent years. However, many agencies maintain a strong security posture overall and the aggregate performance of agencies has increased steadily. The mean rating for agencies as of January 2018 was 725. This is markedly higher than any of the other sector of contractors for the U.S. federal government observed in this study.

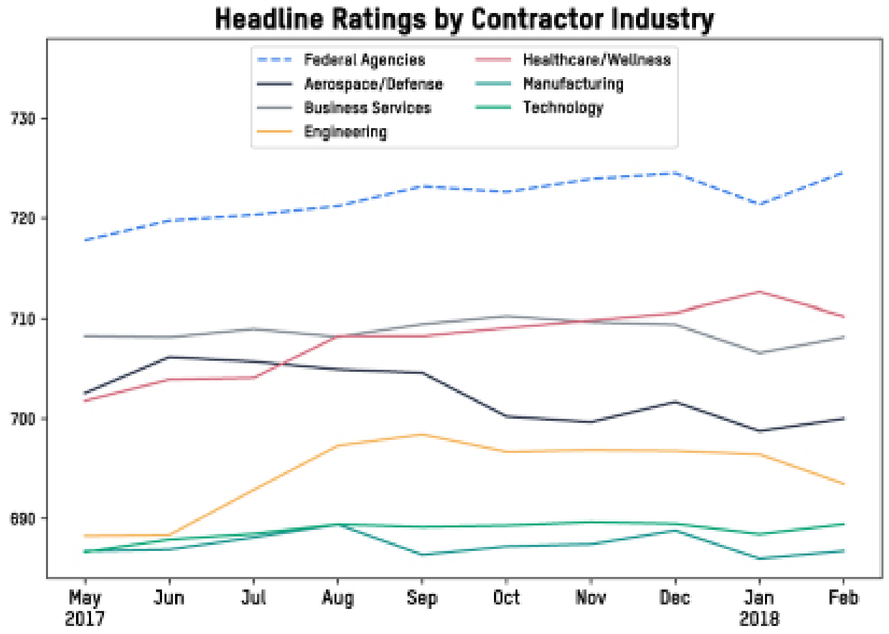


FIGURE 1

The spread of BitSight Security Ratings between federal agencies and contractors as of February 1, 2018.

Within the federal contractor base, Healthcare/Wellness, Business Services, and Aerospace/Defense were the strongest security performers last year relative to other industries, performing between a 700–710 throughout the year, while Engineering, Technology, and Manufacturing were the weakest performers.

BREACH DISCLOSURE RATE

How many U.S. government contractors have experienced a publicly disclosable data breach? Based on the BitSight sample, over 8% of Healthcare and Wellness contractors had disclosed a breach since 2016. Nearly 6% of Aerospace/Defense contractors studied had disclosed a breach in the same timeframe. Not only can these breaches often affect government and private sector employees, they may expose data that is fundamental to national security.

INDUSTRY COMPOSITION

Aerospace/Defense
Aviation | Aerospace | Defense

Business Services
Accounting | Human Resources | Staffing & Recruiting | Management Consulting | Outsourcing

Engineering
Architecture | Construction | Civil Engineering

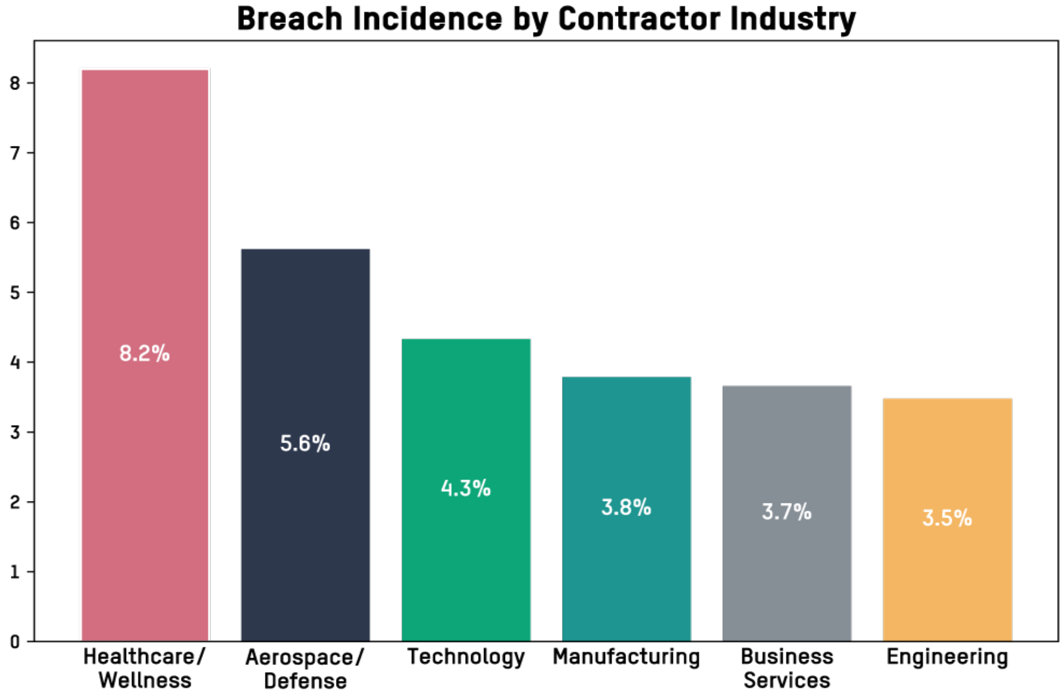
Healthcare/Wellness
Hospitals | Medical Practices | Pharmaceuticals

Manufacturing
Chemicals | Building Materials | Industrial Automation | Machinery | Textiles | Shipbuilding | Electrical

Technology
Computer & Network Security | Software | IT | Medical Devices | Semiconductors | Consumer Electronics

FIGURE 2

The percentage of organizations who have disclosed one or more data breaches from January 1, 2016 to February 1, 2018.



Government agencies continue to press their contractors for timely breach disclosure. For example, the Department of Defense recently passed a rule that requires certain defense contractors to identify and report a suspected or actual cyber incident within 72 hours.[4]

BOTNET INFECTIONS

The President's May 2017 Executive Order on Cybersecurity recognized the critical threat that botnet infections pose to organizations. Botnets can deliver high-volume network attacks and/or distribute spam and malware to organizations, causing operational disruption or the loss of sensitive data. The Executive Order called upon the Secretaries of Commerce and Homeland Security to dramatically reduce botnets across the internet.[5]

BitSight welcomes the U.S. government's focus on this important issue. Through a proprietary sinkhole infrastructure, BitSight is able to observe roughly 80 billion security events per day, many of which are botnet infections. BitSight attributes these infections to organizations and provides a letter grade (A–F) based on the severity and duration of the infections. How an organization prevents or responds to botnet infections is an important indicator of its overall security posture: in previously published Insights reports, BitSight has revealed that an organization receiving a B or lower in this category is more than twice as likely to experience a data breach.[6]

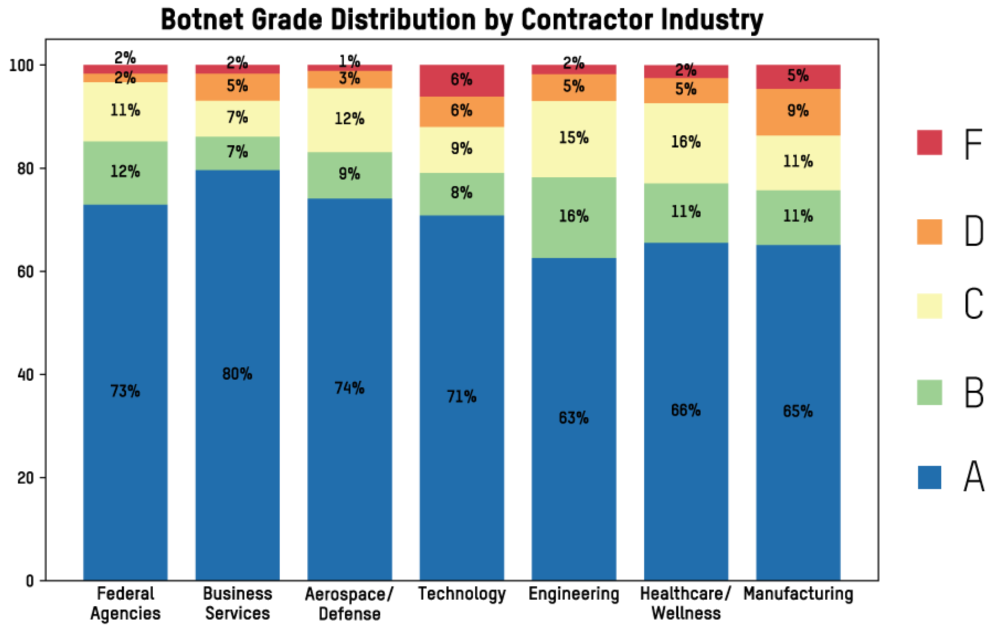


FIGURE 3

BitSight botnet grades (on a scale of A–F) are calculated based on the frequency and severity of botnet infections present on an organization's network. These grades were averaged from January 2017 to January 2018.

BitSight data reveals that the U.S. federal government and its contractor base have pervasive botnet infections on their networks. In fact, a number of contracting sectors -- including Healthcare, Manufacturing, and Engineering—performed at a significantly worse rate than government agencies: 24% of Healthcare/Wellness and Manufacturing contractors have a BitSight botnet grade below B, while 15% of U.S. government agencies perform below a B. This data suggests that these organizations have ineffective security programs in place and may be experiencing ongoing data breaches.

ADHERENCE TO NIST CYBERSECURITY FRAMEWORK

Leveraging data collected externally, BitSight can observe whether organizations are meeting certain best practices established by the U.S. National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF). BitSight examined contractor performance under the "Protective Technology" subcategory of the NIST CSF, particularly "PR. PT-4," which requires that communications and control networks are protected.[7] To determine the effectiveness of an organization's efforts in this subcategory, BitSight considers an organization's open ports exposed to the internet, the strength and use of SSL/TLS encryption across networks, and email security protocols used to prevent phishing attacks, such as SPF and DKIM.

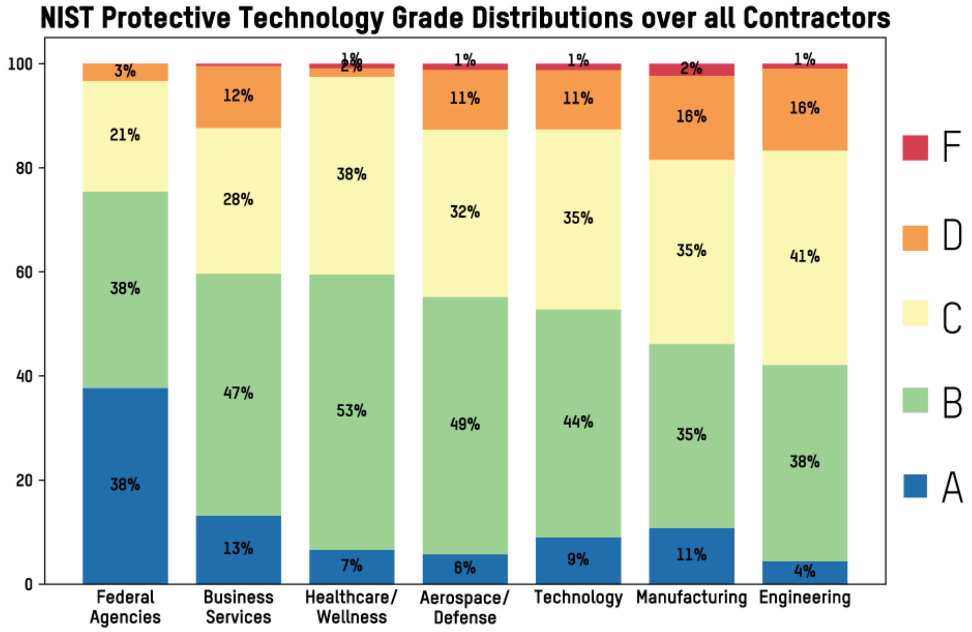


FIGURE 4

The breakdown of BitSight grades for the Protective Technology subcategory of the NIST CSF as of February 1, 2018.

BitSight researchers found that nearly half of the contractors studied fell below a BitSight grade of C, with the Engineering and Manufacturing sectors exhibiting the lowest performance among the sectors. This data suggests that many contractors are not implementing best practices for network security, encryption, and email security. For example, last year's WannaCry ransomware attacks leveraged open services such as Server Message Block (SMB) and Remote Desktop Protocol (RDP).[8] Organizations who had not closed these services properly behind a firewall were left vulnerable.

OUTDATED BROWSERS

According to BitSight's analysis, nearly one in five users for Technology and Aerospace/Defense contractors use an outdated internet browser in the workplace, increasing the contractor company's exposure to compromise. Employees and their organizations are more susceptible to malware if they use outdated or unsupported internet browsers because they do not have the latest security patches in place. High-profile vulnerabilities like Spectre can exploit outdated browsers as an attack to intercept or compromise data.[9] Updating to the latest browser, operating system, or software package is critical to mitigating risks. A previous BitSight Insights report found that organizations running outdated systems were more likely to experience machine compromises.[10]

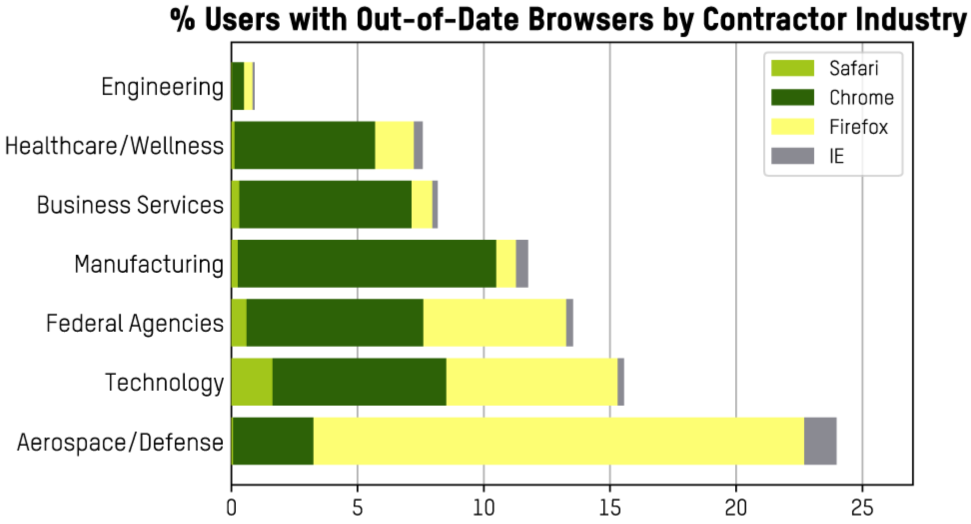


FIGURE 5

The percentage of users in federal agencies and contractor industries with outdated web browsers as of February 1, 2018.

BitSight also finds that U.S. federal agencies have room for improvement in this area as well: nearly 15% of federal agency users rely on outdated internet browsers.

COMMON SERVICE PROVIDERS

The compromise or outage of a technology service provider can have an operational impact on its customers. A recent report by Lloyd's of London and catastrophe modeling firm AIR Worldwide found that the disruption of a major U.S. cloud provider would cause over $19 billion in business losses.[11] How would such an event impact the U.S. government and its contractor base? How does the U.S. government prepare for this risk?

BitSight is able to identify a common set of fourth party relationships and service providers used amongst a given set of companies. Across the sample of contractors studied, BitSight researchers were able to identify nearly 2,000 common service providers, with a significant concentration among a handful of key providers.

Given the high dependency rates on certain service providers, an outage of top hosting, email, and DNS providers would likely impact many, if not all federal agencies in some manner. Understanding these dependencies and potential consequences is crucial not only for contractors themselves, but for federal agencies who may also be affected.

CONTRACTOR DEPENDENCY ON SERVICE PROVIDERS

Hosting
GoDaddy 40%
Amazon 40%
Rackspace 32%

Email
Microsoft Azure DNS 69%
Microsoft Exchange Online 63%
Office 365 Mail 59%

DNS
Network Solutions DNS 48%
GoDaddy DNS 44%
Amazon Route 53 22%

RECOMMENDATIONS

1. Make third party cyber risk management a key management priority for federal agency leaders.

U.S. government contractors, subcontractors, and other third parties can be the cause of significant losses of government data. Agency leadership must ensure that these organizations are protecting the sensitive government data with which they have been entrusted. Political, technology, and civil service leaders within an agency all must be involved in addressing this risk.

2. Adopt robust commercial practices for third party risk management, including cyber diligence and continuous monitoring.

In improving their risk management initiatives, agencies should consider methods that have gained widespread adoption in the commercial sector, including performing cybersecurity diligence on contractors and subcontractors prior to entering into a business relationship and continuously monitoring the security posture of these organizations during the lifetime of the relationship. These methods should include collecting quantitative, objective performance measurements rather than relying exclusively on check-the-box compliance questionnaires. Adopting these methods will enable the U.S. government to close the cybersecurity performance gap with its contractors and reduce the likelihood and severity of data breaches, outages, or other cyber events involving third party actors.

3. Require prime contractors to continuously monitor their subcontractors.

In recent years, certain agencies within the U.S. federal government have ordered prime contractors to bear the responsibility for subcontractor cybersecurity by requiring the primes to place legal requirements on their subcontractors with respect to cybersecurity and breach disclosure. These are known as “flow down” provisions. While these provisions create legal requirements for subcontractors to meet certain cybersecurity standards, they do not require the prime contractors to continuously monitor their supply chain. As a result, federal requirements fall far short of commercial best practices. Federal agencies should address this gap and require continuous monitoring.

4. Don’t neglect the risk posed by technology service and cloud providers.

A severe disruption affecting technology service providers could have a widespread impact on U.S. government contractors and subcontractors, potentially imperiling the missions that they are performing on behalf of their federal agency customers. In addition to achieving greater oversight of the cyber risk posed by contractors, it will be critical for the U.S. government to also understand how risk may also trickle down from common vendors, platforms, and technologies used by contractors themselves.

METHODOLOGY

BitSight analyzed 1,212 contractors and 122 federal agencies in this study. Contractors studied were randomly selected from usaspending.gov, with a minimum of $10,000 obligated from the U.S. government. The average contract size of this sample was $1.5 million. Headline Security Rating data spanned from May 1, 2017 to February 1, 2018. Breach Incidence by Contractor Industry data spanned from January 1, 2016 to February 1, 2018. BitSight records publicly disclosed data breaches from verifiable news sources and government portals, and by filing Freedom of Information Act requests. Note that various jurisdictions have differing breach reporting requirements. Data on BitSight botnet grades, NIST Protective Technology grades, out of date browser versions, and common service providers were processed on February 1, 2018. Out-of-date browsers are defined as installations that are not on the latest available version at the time of observation.

REFERENCES

1. Research Federal Government Contractors http://government-contractors.insidegov.com/

2. "Top Five Government Contractor Cybersecurity Considerations for 2018," Morrison and Foerster, January 2018 https://www.lexology.com/library/detail.aspx?g=c4fbe9c3-1403-433f-abeb-fb739a17729c

3. BitSight Insights: The Buck Stops Where?, September 2017 https://www.bitsighttech.com/hubfs/Insights/The%20Buck%20Stops%20Where_%20Assessing%20the%20Cybersecurity%20Performance%20of%20the%20Finance%20Supply%20Chain.pdf

4. "Contractors Must Contend With New Cybersecurity Rule," Ebner and Sanchez, January 2018. http://www.nationaldefensemagazine.org/articles/2018/1/4/contractors-must-contend-with-new-cybersecurity-rule

5. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017 https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

6. BitSight Insights: Beware the Botnets, April 2015 https://www.bitsighttech.com/hs-fs/hub/277648/file-2726147033-pdf/Insights/BitSight_Insights_Beware_the_Botnets.pdf?t=1513633447234

7. National Institute of Standards and Technology Framework for Improving Critical Infrastructure, February 2014 https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

8. Everything you need to know about the WannaCry / Wcry / WannaCrypt ransomware, Hunt, May 2017 https://www.troyhunt.com/everything-you-need-to-know-about-the-wannacrypt-ransomware/

9. Barkly Blog: A Clear Guide to Meltdown and Spectre Patches, January 2018 https://blog.barkly.com/meltdown-spectre-patches-list-windows-update-help

10. BitSight Insights: A Growing Risk Ignored, June 2017 https://www.bitsighttech.com/hubfs/Insights/BitSight%20Insights%20-%20A%20Growing%20Risk%20Ignored%20-%20Critical%20Updates.pdf

11. Lloyd's and AIR Worldwide, Cloud Down: Impacts on the US Economy, January 2018 https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down