Best Cybersecurity Practices for Companies, Post Van Buren

Mary Riley

Old Dominion University

COVA CCI Undergraduate Cybersecurity Research Program

Fall Semester 2021

Contents

I. Introduction

Imagine this scenario: you are a small business owner, and you've just been informed of a network security breach. In your Zoom meeting with the IT Department, you learned the details: network activity logs revealed aberrant behavior after hours. Threat actors accessed systems containing sensitive information and downloaded copies of key files containing company trade secrets, market strategies, and customer data – all within a matter of minutes. Immediately, you review the consequences of the breach in your mind: reputational harm, monetary loss, and potential lawsuits. You ask the IT professional about the root cause of the breach. Was it a single individual or a syndicate that pulled off the hack? How did the threat actors manage to bypass the company's firewall and network intrusion detection system?

Then you receive the news. The hacker was a former employee whose login and password credentials were still active. As is often the case with smaller businesses, your former employee wore many hats in her role at your company. As a trusted insider, she had access to confidential and proprietary information stored on network drives and knew which times (day or night) were best to try accessing the network without being noticed. Once logged in, she knew exactly how to locate and steal data in a minimum amount of time before logging out.

This example is not just an imagined hypothetical. Insider threat risk management is a growing challenge for companies of all sizes, with rising reports of current or former employees accessing company networks to engage in corporate espionage or steal customer data for personal gain.[1] The Verizon 2021 Data Breach Investigations Report (DBIR), in its analysis of 5,258 confirmed breaches (out of 29,207 security incidents in 2020), determined that 85% of

[1] See, e.g., Brook, Chris. "Software Company Claims Ex-Employee Stole Data, Clients Before Exit," (June 4, 2021). *Data Insider* (Digital Guardian Blog; Burgess, Christopher. "Former employee visits cloud and steals company data," (March 21, 2018). CSO (IDG Communications).

breaches involved a human factor and 61% of breaches involved credential data.[2] Over 30% of security incidents stemming from privilege misuse go undiscovered for months or even years.[3] Similar to cases of employee theft or embezzlement of physical assets,[4] many company network security breaches are attributable to a trusted insider who, for a variety of reasons, is motivated to steal intangible assets such as intellectual property, strategic market information, or customer data.[5] At the root of these incidents is an employee who abuses that trust.

An employer has three options for dealing with such an employee: (1) terminate the employee;[6] (2) take legal action (although ongoing litigation risks further reputational damage to the company); and/or (3) turn the matter over to law enforcement for criminal prosecution. Whether a company should pursue legal action depends on the circumstances of the case. Civil and criminal remedies under state law for unauthorized access and misuse of computer resources vary, depending on the state in which the act occurred. Nevertheless, all fifty states have enacted cybercrime statutes, with at least some also providing private rights of action for civil relief.[7] Unfortunately, the fallout from data breaches may be viewed in several ways. Businesses are often both the victim and defendant in data breach cases. Business partners, consumers, and

[2] Verizon 2021 Data Breach Investigations Report (DBIR) SMB Snapshot (DBIR Snapshot) at 4.
[3] DBIR Snapshot, *supra* note 2, at 7.
[4] See, e.g., Bohr, Nick, "County Clare Bookkeeper accused of embezzling $92,000," (May 17, 2019), WISN.com; Jenco, Melissa, "Ex-Dixon Comptroller Gets Nearly Twenty Years for Theft," (February 15, 2013), Chicago Tribune.
[5] *Insider Threats and Commercial Espionage: Economic and National Security Impacts* (May 2021). Intelligence and National Security Alliance (INSA), Insider Threat Subcommittee Report.
[6] Of course, job termination is not an option when the cyberattacker is a former employee.
[7] See, e.g., Va. Code § 18.2-152.12 (2021); 720 ILCS 5/17-51(b)(6); *Computer Crime Statues*, National Conference of State Legislatures. See also, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1597 (2003) (hereinafter "Cybercrime's Scope"). Kerr points out that different states use different terminology when defining unauthorized access, misuse, and the requisite *mens rea* for being found culpable.

other plaintiffs impacted by the data breach may bring civil claims against companies based on common law theories of legal liability and/or statutory remedies.[8]

Under federal law, companies may look to the federal cybercrime statute, the Computer Fraud and Abuse Act (CFAA),[9] for civil redress and criminal sanctions. The CFAA imposes criminal[10] and civil[11] liability upon a person who, "without authorization or exceeding authorized access," knowingly accessed or damaged a protected computer. The CFAA has commonly been used by companies to hold a current or former employee liable for accessing a company's network to misuse, steal, or destroy company assets, which includes company's proprietary information and customer data.[12] Since virtually all work computers are connected to the internet, employee misconduct involving unauthorized access of a company's network falls within the CFAA's reach, irrespective of where the bad acts occurred.[13]

However, a split grew over time in how the federal courts interpreted the meaning of the term "unauthorized access," both in terms of "access without authorization" and an act which "exceeds authorized access" under the CFAA.[14] The First, Fifth, Seventh, and Eleventh federal circuits broadly construed the term "unauthorized access" to encompass instances where an

---

[8] See., e.g., Hooker, Michael, and Jason Pill. "You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*." The Florida Bar Journal* (July/August 2016), pp. 42-40. Exactly what constitutes a showing of harm sufficient to establish standing to bring a data breach claim is not always clear. However, in cases of successful data breach claims, the courts are free to also consider punitive damages when determining sanctions against an employee for wrongfully accessing an employer's network or misusing company data. See, Murray, Maxwell, *Stand or Sit? Article III Standing in Cases of Data Breach: A Uniform Solution*, 5 ST. THOM. J. OF COMPLEX. LIT. 46 (2019); Fisher, John A. *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 4:215, 238 (2013).

[9] 18 U.S.C. §1030 (Pub. L. No. 99-474, 100 Stat. 1213 (1986). The present version of the CFAA expands upon the earlier version enacted under the Comprehensive Crime Control Act of 1984 (Pub. L. No. 98-473, 98 Stat. 1837). See Kerr, Cybercrime's Scope, *supra* note 7, at 1598.

[10] 18 U.S.C. §1030(c).

[11] 18 U.S.C. §1030(g).

[12] See, e.g., *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[13] O'Connor, Michael J. *Standing Under the Computer Fraud and Abuse Act*, 124 PENN STATE L. REV. 743, 745 (2020), (citing to Orin S. Kerr, *Cyberspace & the Law: Privacy, Property, and Crime in the Virtual Frontier: Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1564 (2010)).

[14] It was precisely this split in the courts that made the *Van Buren* case ripe for review.

employee accessed a company computer for an improper purpose, in violation of an employer's policies. In contrast, the Second, Third, Fourth, Sixth, Eighth, Ninth, and Tenth federal circuits construed the term "unauthorized access" more narrowly, such that employees who accessed a network for improper purposes were not found liable under the CFAA.[15]

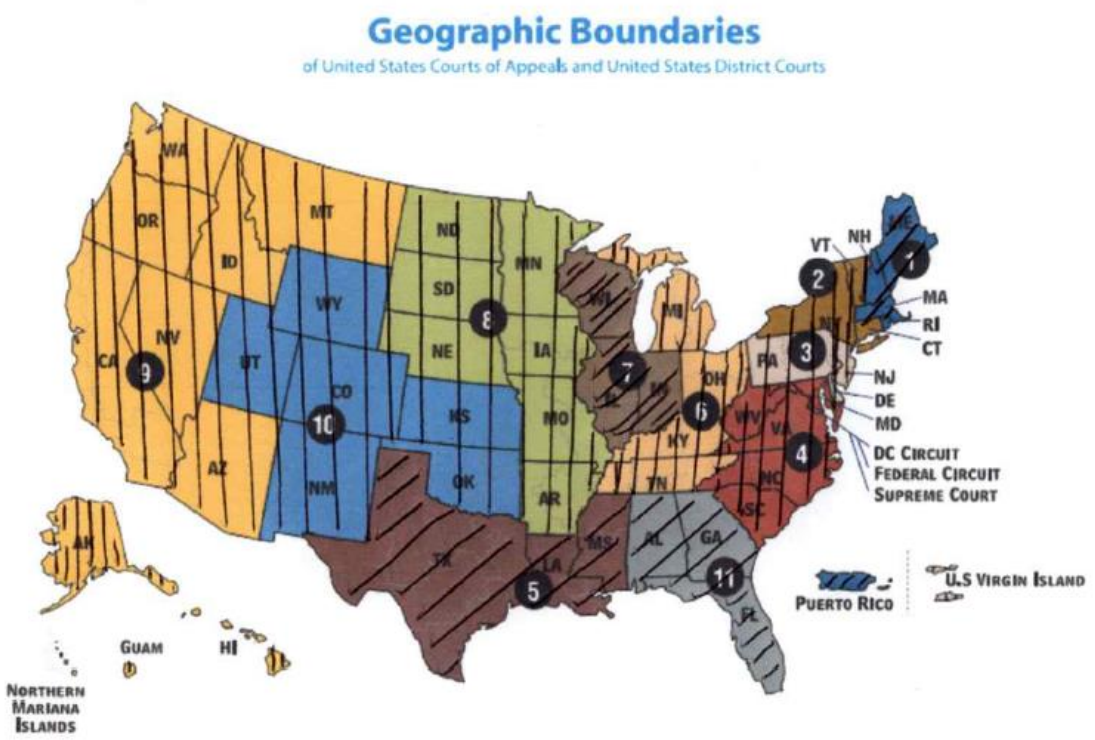


Figure 1. The federal circuits which ruled broadly are shown with diagonal lines, and the federal circuits which ruled narrowly are shown with vertical lines.

The implications of this split in the federal circuits was that whether a defendant would be found liable under the CFAA for accessing a computer without authorization depended on

[15] See Figure 1 for an illustration of the federal circuits which interpreted the term "unauthorized access" broadly (using horizontal stripes) and the federal circuits which interpreted the term narrowly (using diagonal stripes). The federal circuits which construed the term "unauthorized access" under the CFAA broadly tended to focus on whether the defendant exceeded the scope of authorization a person or employer granted to the defendant, or whether the grant of authorization was predicated on proper purpose. The federal courts which construed the term narrowly tended to examine whether the defendant accessed all, or a portion of, a computer to which he never had authorization to access, without taking intent, or access for an improper purpose, into account.

which federal circuit had jurisdiction over the case, which also made this issue ripe for review by the Supreme Court of the United States.[16] The recent Supreme Court decision in *Van Buren v. United States*,[17] which addressed the split in the federal circuits and interpreted the meaning of "exceeds unauthorized access" under the CFAA,[18] has undercut the CFAA's ability to hold individuals civilly and criminally liable for their bad acts. The Supreme Court narrowed the meaning of the term "exceeds unauthorized access" in *Van Buren* to such an extent that the plain meaning of this term (to most people, in everyday language) no longer applies.[19]

A. Best Practices post *Van Buren* era

This paper explores the ramifications of the *Van Buren* decision on employers' cybersecurity policies and best practices. The *Van Buren* decision interprets the CFAA to only apply to a narrower class of employee misconduct, which is confounding for companies because it means that some obvious, commonsense instances of employee misconduct do not fall within the purview of the CFAA. The only clear signal the *Van Buren* decision provides is that, unless Congress acts to amend the CFAA, companies cannot rely on the CFAA to punish trusted insiders who access company networks for an improper purpose because the terms "exceeds unauthorized access" and "without authorization" are synonymous with "no access at all." Under *Van Buren*, an employee is only liable under the CFAA if the facts show the employee, similar to an outside hacker, literally broke into a portion of the network which the individual had no authority to access. The *Van Buren* decision also requires companies to tailor cybersecurity solutions to fit their current, real-world circumstances and risk posture. Since there

[16] Petition for Writ of Certiorari, *Van Buren v. United States*, cert. granted (U.S. April 20, 2020) (No. 19-783) (hereinafter *Petition for Writ*). Throughout this paper I will refer to SCOTUS as the U.S. Supreme Court.
[17] *Van Buren v. United States*, 593 U.S. ___, 141 S. Ct. 1648, 1652, 1662 (2021) (hereinafter *Van Buren*).
[18] 18 U.S.C. §1030(a)(4).
[19] *Van Buren*, *supra* note 17 (Thomas, J., dissenting).

is no silver bullet or "one and done" solution for managing cybersecurity risk, a company's adoption of a well-honed risk management approach can minimize its cybersecurity risk to reasonable levels, irrespective of the current legal and jurisprudential landscape. As part of a review of best cybersecurity practices, this paper will recommend: (i) general cybersecurity measures all companies may adopt, irrespective of a company's size, budget, or resources; and (ii) cybersecurity measures to address specific concerns of businesses based on their size as well as their resource and budgetary constraints.

II. Background: The United States Supreme Court and the *Van Buren* Decision

The facts of the case presented in *Van Buren* are not in dispute. In *Van Buren*, a former Georgia police officer (Van Buren) accepted bribes from a man, who was an informant for the FBI, to run a driver's license plate search on an individual to find out whether that person was an undercover officer. Additional context is provided in Daniel Shin's analysis of *Van Buren*:

> Based on his prior relationship with Albo, Van Buren thought Albo could provide him with a personal loan without issue. Unbeknownst to Van Buren, Albo recorded their conversations and turned over the audio recordings to a law enforcement detective, alleging that Van Buren was "shak[ing] him down for his money." *Id.* at 1997 … the [FBI] sting operation entailed Albo giving Van Buren cash in exchange for checking whether a woman from a strip club was an undercover officer. Over the course of several meetings, Van Buren agreed to search the woman's license plate in the police database in exchange for $15,000. Unbeknownst to Van Buren, Albo provided a fake license plate number that was created by the FBI.
>
> The day after he ran the fake license plate number using his patrol-car computer, Van Buren was interviewed by law enforcement authorities, and he subsequently admitted running the license plate number in exchange for money.[20]

[20] For an in-depth review of the background and analysis of the *Van Buren* case, see D. Shin, "U.S. Supreme Court limits the scope of criminal violation under the Computer Fraud and Abuse Act," *Cybersecurity and Information Security Newsletter* Issue 8 (June 30, 2021), Center for Legal and Court Technology, College of William and Mary (hereinafter D. Shin, CFAA).

By doing so, Van Buren violated a departmental rule prohibiting employees from using or accessing work computers for non-law enforcement purposes.[21] The FBI apprehended him and charged him with, among other federal crimes, a felony under the CFAA.[22] Officer Van Buren was convicted[23] under the CFAA, and his conviction was subsequently affirmed[24] by the 11th Circuit Court of Appeals.[25]

Van Buren then petitioned the Supreme Court to hear the case, presenting the legal question of whether a person who is authorized to access information on a computer for certain purposes violates the CFAA if he accesses that information for an *improper* purpose.[26] The Supreme Court determined the split in the federal circuits over what constitutes "unauthorized access" under the CFAA was sufficiently significant to grant certiorari and agreed to review the case.[27] Counsel for Van Buren argued before the Supreme Court that he was wrongly convicted under the CFAA because: (1) he was authorized to access the driver's license plate database in the first place; and (2) the meaning of "exceeds unauthorized access" under the CFAA only refers to individuals who access a computer to which they have no authorized access, and not to those who misuse their access for an improper purpose.[28] In contrast, counsel for the U.S. government argued that the meaning of "unauthorized access" was broader and covered the police officer's misuse of computer resources and information since "authorized access" implied a limit to what a person could do, even with general authority to access a computer or system.[29]

---

[21] Ibid, at 2.
[22] This was not the police officer's only crime. He was also terminated from his employment.
[23] *United States v. Van Buren*, No. 1:16-cr-00243-ODE-JFK-1 (N.D. Ga. May 3, 2018).
[24] *United States v. Van Buren*, No. 18-12024 (11th Cir. Oct. 10, 2019).
[25] D. Shin, CFAA, *supra* note 20, at 2.
[26] *Petition for Writ*, *supra* note 16, at 6.
[27] Order No. 19-783, *Orders of the Court* (Monday, April 20, 2020) at 3.
[28] *Brief for Petitioner*, On Writ of Certiorari to the United States Court of Appeals for the Eleventh Circuit (July 1, 2020).
[29] *Brief for Respondent*, On Writ of Certiorari to the United States Court of Appeals for the Eleventh Circuit (August 27, 2020).

A. Implications (Arguments for Petitioner and Government)

Several amicus briefs, both in support of Van Buren and of the U.S. government, were filed in this case,[30] with diverse and far-reaching arguments presented. Amicus briefs in support of the government's position included arguments that narrowing the definition of "exceeds authorized access" under the CFAA would make it difficult to protect against and prosecute insider threats, and law enforcement departments would be severely hampered in their ability to do their work because every law enforcement network, system, database, and even file would have to be locked down to minimize insider threats.[31] Principal arguments in amicus briefs against supporting a broader definition of "exceeds authorized access" under the CFAA included concerns about overcriminalization, turning the CFAA into a private criminal law, statutory vagueness, and the chilling effects such an interpretation would have on security professionals' research activities.[32] This review only touches upon a few of several arguments both for and against the adoption of a broad interpretation of the CFAA.

---

[30] An *amicus curiae* (literally translated as "friend of the court"), is a brief filed by a non-party which provides analyses and insights that have bearing on the present case, and makes additional arguments for the Supreme Court's consideration to decide how to rule on the issue of law presented in the case. Amicus briefs often argue on grounds of public policy for the Supreme Court to make its ruling, but there may be competing public policy interests for the Supreme Court to consider when ruling one way or the other.

[31] See, e.g., *Brief of the Federal Law Enforcement Officers Association as Amicus Curiae in Support of Respondent* ("If the CFAA is interpreted not to criminalize misuse of data to which technical access has been granted, law enforcement will be deprived of a powerful tool — in some cases the only tool — to deter and punish unauthorized misuse of vital criminal intelligence systems and databases."); Brief of Karen Heart and Anthony Volini of CIPLIT in Support of Respondent ("There is no reason why traditional notions of consent to use of property should not be applied to criminal prosecutions under the CFAA, which may be viewed as tantamount to a state law theft charge.");

[32] See, e.g., *Brief of the National Association of Criminal Defense Lawyers as Amicus Curiae in Support of Petitioner* ("adopting an expansive reading of the CFAA would instantaneously transform common, seemingly innocuous instances of computer misuse—such as utilizing a work computer to (citing *Nosal*) 'chat[] with friends,' 'shop[],' or 'watch[] sports highlights'—into federal crimes throughout the entire nation … '[T]his would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime.'"); *Brief of Amici Curiae Computer Security Researchers, Electronic Frontier Foundation, Center for Democracy & Technology, BugCrowd, Rapid7, Scythe, and Tenable in Support of Petitioner* ("Under the government's broad interpretation of the CFAA, standard security research practices—such as accessing publicly available data in a manner beneficial to the public yet prohibited by the owner of the data—can be highly risky.").

B. U.S. Supreme Court Decision

The Supreme Court subsequently reversed (6-3) and remanded the case, adopting the narrower view and holding that the CFAA only applies when a person "accesses a computer with authorization but then obtains information located in particular areas of that computer—such as files, folders, or databases—that are off-limits to him. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them."[33] In its opinion, the Supreme Court agreed that a broad interpretation of the term "exceeds authorized access" would result in the criminalization of many everyday computer activities:

> To top it all off, the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity … If the "exceeds authorized access" clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals. Take the workplace. Employers commonly state that computers and electronic devices can be used only for business purposes. So on the Government's reading of the statute, an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA.[34]

The Supreme Court also opined that Congress' amending the CFAA in 1986 to remove references to purpose-based reasons for accessing a computer tended to work against the government's argument that the term "exceeds authorized access" under the CFAA should be extended to cover access for an improper purpose, and suggested that the remedy lies with Congress, and not the Court, to change the language of the CFAA.[35]

---

[33] *Van Buren*, *supra* note 17, at 1662.
[34] Ibid, *supra* note 17, at ___. Notably, the Supreme Court extensively cited Orin Kerr's legal scholarship and his submitted amicus brief (see, Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Petitioner) and generally agreed with those arguments supporting the petitioner's position.
[35] Ibid., *supra* note 17 at ___.

III. Best Cybersecurity Practices for Companies re: Unauthorized Access: Tools That Work

Until Congress decides to amend the CFAA,[36] the only guidance *Van Buren* provides for businesses is that: (1) there is no recourse under the CFAA against trusted insiders when they misuse or abuse pre-existing authorized access to steal company data; and (2) company systems need to be "locked down" and closely managed to monitor both insider and outsider behavior, since the only recourse a company would have against a trusted insider under the CFAA would be in instances where the trusted insider accessed parts of the network which the insider was clearly *never* granted authorization to access. With the bar now raised markedly higher for a company to recover against trusted insiders under the CFAA, businesses need to revisit their cybersecurity risk management and recalibrate their cybersecurity risk postures in light of the treatment of insider threats under *Van Buren*.

A. Zero-Trust Principles and Architecture

From a risk management perspective, the most practical way to ensure company networks are adequately locked down is to implement zero-trust principles and architecture to protect assets and users from both insider and external threats.[37] Unlike traditional, perimeter-driven cybersecurity models, the zero-trust cybersecurity model is location-agnostic[38] and recognizes that: (i) most enterprise networks have grown in complexity to the point where there

[36] At this time of this writing, only legislative action that appears to have been taken in response to *Van Buren* is the introduction (on June 24, 2021, three weeks after *the Van Buren* decision) of the Study on Cyber-Attack Response Options Act (S.2292 – 117th Congress (2021-2022). However, the purpose of this bill is only to require the Department of Homeland Security to "study the potential consequences and benefits of amending the Computer Fraud and Abuse Act to allow private companies to take proportional actions in response to an unlawful network breach."

[37] Scott Rose (NIST), Oliver Borchert (NIST), Stu Mitchell (Stu2Labs), Sean Connelly (DHS). "Zero-Trust Architecture." NIST SP 800-207 (August 2020) (hereinafter Zero Trust Architecture).

[38] By "location-agnostic", I mean that the zero-trust model assumes that: locations inside the network are no more trustworthy than locations outside the network; and (2) protection is focused on enterprise assets and users since an attacker is equally likely to be within the network as outside of it.

is no one perimeter to defend; and (ii) the most vulnerable part of any network is the human part, since humans can be tricked, cajoled, compelled, or coerced into causing a network security breach.[39] Since zero-trust assumes an attacker may already be within a network, no trust is the default posture and cybersecurity is implemented at the transaction level by following the principle of least privilege.[40]

Zero-trust architecture works along three dimensions: (1) protecting the network (both internally and externally); (2) restricting the lateral movement of an attacker once in the network; and (3) restricting the movement of an attacker by integrating zero-trust principles between components that communicate with one other within the network ecosystem.[41] Multi-factor authentication (MFA) is a core value of zero-trust security, since a user must provide several pieces of information to authenticate at (i) every new interface and (ii) the beginning of every session.[42]

[39] See, National Initiative for Cybersecurity Education (NICE), "Cybersecurity is Everyone's Job," (October 2018), NICE Working Group Workforce Management Subgroup, at 4 (hereinafter the NICE Guidebook).
[40] Zero Trust Architecture, *supra* note 37, at 1. In a sense, the principle of least privilege is a concrete form of zero-trust principles in action: a user is only granted access to a network system or resource (which may contain assets or sensitive data) to the extent the user has a legitimate reason to have any access privilege.
[41] While this is beyond the scope of this paper, there is a lot here that merges into the practical, "tools that work" section to follow. The big picture is that, although the default posture has been that insiders are trusted while externals are not, the new default posture under zero-trust principles is that no one is trusted, requiring verification and authentication each time, each session. Ross, Ron "When Perimeter Defenses Are Not Enough: How Multidimensional Protection Strategies Can Provide True Cyber Defense-in-Depth." (April 21, 2020), Presentation, NIST Information Technology Laboratory, Computer Security Resource Center.
[42] Zero-Trust Architecture, *supra* note 37, at 7.

Zero Trust Principles and Architecture
• Cybersecurity controls are implemented both inside and outside of the network. • Zero trust is the default assumption. • Zero trust assumes that an attacker may already be inside the network. • User authentication happens at every transaction (file, folder, subdirectory, drive, or system) as a user traverses a company network. • Cybersecurity is location-agnostic, not related or tied to the network perimeter. • Zero trust principles and architecture generally restrict an attacker's movement across a network, since least access principles (correctly implemented at the transaction level) ensure that an attacker cannot automatically access all assets or data on the network.

B. Best Cybersecurity Practices For All Companies (Any Size)

There are several best cybersecurity practices that companies of any size can adopt to prevent unauthorized access to company assets, resources, and systems:

Access Control. Access control means the process of granting or denying specific requests to: (i) obtain and use information or related systems or services; or (ii) enter specific physical facilities.[43] This is accomplished by following the principle of least privilege to determine a user's rights to access company networks, systems, drives, directories, folders, or files containing assets or data. Typically access control is implemented granularly, such as granting users only the minimum access required to perform their jobs.[44] Access to resources on a network can also be "time-bound" such that a user may only be granted access to a network drive, folder, or file during a company's standard work hours (9 a.m. to 5 p.m.) while not permitting that same user access outside of that time period.[45] By centralizing user, system, and

[43] Nieles, Michael, Dempsey, Kelley, and Pillitteri, Victoria Yan (2017). "An Introduction to Information Security." NIST Special Publication 800-12 (Rev. 1), at 59 (hereinafter NIST InfoSec Introduction).
[44] Several examples can be used to illustrate this principle. A user may be granted read-only, write, or execute privileges to a file. A user granted execute-level access to a file is also able to view and edit the file, while a user who only has read-only access cannot edit or execute the file. Similarly, an employee may only be granted access to the functions and features of a system as necessary and appropriate for their role.
[45] Even further, user access can be configured in such a way that a user's (unauthorized) attempts to access a file after business hours would result in an "access denied" message and would show up on a network activity log.

policy management, a company's network administrator has greater ability to track users to ensure they have role-appropriate access levels to systems, resources, and data, and that when users leave the company, access credentials are promptly revoked and deleted from the network.

Access Control Best Practices
• Access Control is a concrete form of zero-trust principles in action. • Employees should only be granted the minimum amount of access required for them to do their jobs. • Managers should determine and document the required minimum access for their teams. • Network administrators should work with managers and HR to align on appropriate access. • Profiles, credentials and passwords of employees who leave the company should be deactivated within 24 hours and removed from the company network.

Data Exfiltration Prevention. Even companies with strong access control policies in place should also implement data exfiltration prevention measures to prevent both unintentional and intentional removal of data from the company network.[46] Companies of all sizes can utilize data loss prevention (DLP) tools to prevent data exfiltration. For example, some DLP tools are designed to work with email applications to monitor and prevent outbound emails potentially containing sensitive company information from being successfully transmitted to an email address outside the company.[47] USB ports on company laptops can be disabled so that an employee cannot, for example, copy company files from a network drive to a thumb drive. Similarly, company systems can be configured to block employee access to public file-sharing services and social media sites, where company data can be uploaded out of the network within a

[46] It is important to note here that not all data exfiltration occurs with malicious intent. For example, a well-meaning employee who saves a copy of a work spreadsheet to a memory stick to take it home and continue working on it (against company policy) is deliberately removing data from the company's network. Even though the employee's intentions are good, if the memory stick is misplaced or lost the company might sustain a cybersecurity breach as a result.

[47] For example, G Suite tools. Many applications come with built-in data exfiltration alert and prevention systems.

few clicks of a mouse.[48] Although DLP tools cannot detect relatively sophisticated data exfiltration techniques, DLP tools are a relatively inexpensive solution for most businesses.[49]

Since virtually all employees require at least a minimal level of access to company networks in order to do their jobs, employers must develop policies that clearly define what constitutes prohibited data exfiltration, and then, as part of building a cyber-secure workplace culture, implement the policies with training sufficient for employees to understand the company's expectations and requirements.[50] Companies should periodically review how employees use technology to perform their work and determine best practices to prevent data exfiltration accordingly,[51] and advise employees their work computer usage is monitored to deter employee misconduct using company resources and equipment.[52]

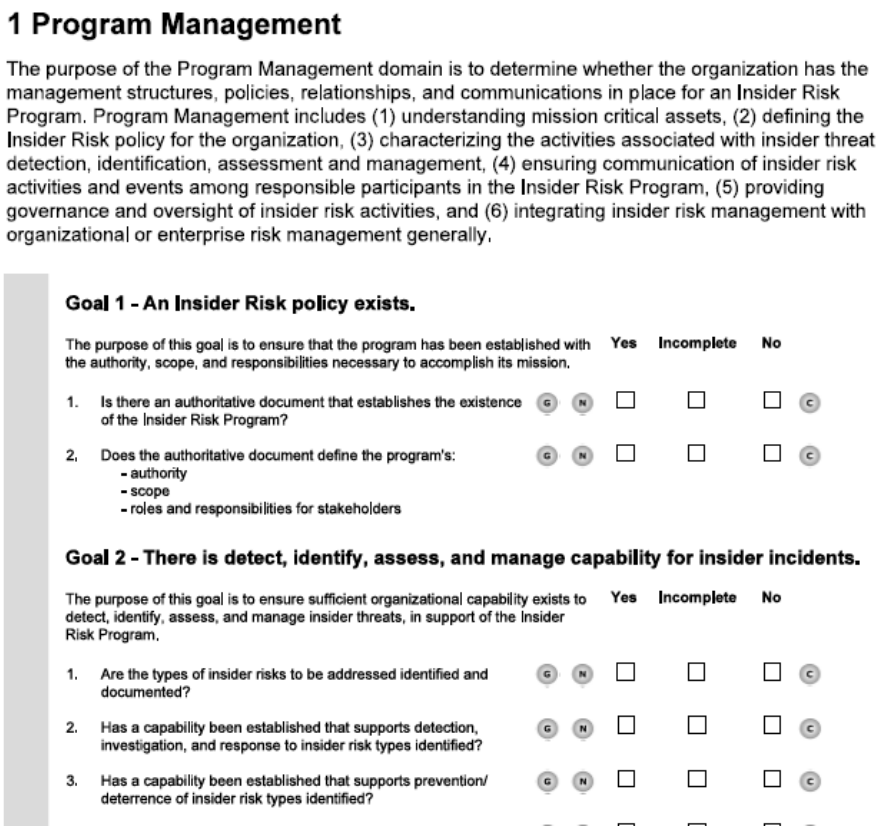
Data Exfiltration Prevention Principles and Best Practices
• Data Exfiltration Prevention means all measures used to prevent the unauthorized removal of information or data from company networks. • Company firewalls should be configured to block risky websites. • Policies should be developed to clearly define what constitutes prohibited data exfiltration. • Employees should receive adequate training on data exfiltration prevention and be informed of the DLP tools and methods the company has put into place to automatically prevent data exfiltration.

[48] See, Exfiltration Over Web Service: Exfiltration to Cloud Storage.
[49] For example, steganography is a technique by which data can be hidden in image files, including streaming video files, by altering and hiding it.
[50] NICE Guidebook, *supra* note 39, at 6.
[51] See, e.g., Kaplan, Dan. "Preventing Data Exfiltration: Definition, Examples and Best Practices," (June 9, 2020). This article outlines several best practices to prevent data exfiltration, using a multi-dimensional approach: (1) block unauthorized communication channels; (2) prevent phishing attacks; (3) systematically revoke systems and data access for former employees; (4) educate employees on data loss prevention (especially policies prohibiting copying data to personal devices, where an employee might, with the best of intentions, do so in an effort to continue working off-hours); (5) identify and redact sensitive data; (6) set a clear bring-your-own-device (BYOD) policy; (7) identify malicious and unusual network traffic; (8) implement data encryption and backup processes; and (9) to the greatest extent possible, automate DLP plans.
[52] The federal Electronic Communications Privacy Act of 1986 allows businesses to monitor employees' electronic communications as long as there is a valid business purpose for doing so. U.S.C. §§ 2510-2523.

Insider Threat Risk Management. In addition to having robust access control and data exfiltration prevention policies, companies can further protect assets and users by developing an insider threat risk management program. The federal Cybersecurity and Infrastructure Security Agency (CISA) has several resources for companies to comprehensively self-assess and manage insider threat risk.[53] CISA defines an insider threat as the potential for an insider to use, intentionally or unintentionally, their access or understanding of an organization to harm that organization.[54] Companies should be aware that many time-honored, common-sense policies developed to manage employees' handling of *physical* data and assets also serve to minimize insider threat risk. Insider threat risk management to protect company assets and users on a network is no different.[55] Existing policies and procedures governing access to, handling, and disposal of company assets, information, and data should be periodically reviewed and updated in accordance with the company's current cybersecurity risk posture.

Similarly, the CISA's Insider Threat Self-Assessment Tool provides a company with a customized assessment and evaluation of its insider threat security risk posture, and recommendations on what additional controls are needed to improve their risk posture and minimize insider threat risk.[56]

[53] See, CISA website, Insider Threat Mitigation webpage, at https://www.cisa.gov/insider-threat-mitigation.
[54] CISA website, Defining Insider Threats webpage.
[55] For example, controls in place to safeguard physical copies of sensitive data, such as employee "clean desk" policies or having locked disposal bins, are meant to secure physical copies of reports, statements, or presentation decks containing a company's confidential or proprietary information. Employees' compliance with these data handling and disposal policies minimizes the risk of improper access or disposal of data, so the end result is a mitigation of insider threat risk.
[56] See Figure 2.



1 Program Management

The purpose of the Program Management domain is to determine whether the organization has the management structures, policies, relationships, and communications in place for an Insider Risk Program. Program Management includes (1) understanding mission critical assets, (2) defining the Insider Risk policy for the organization, (3) characterizing the activities associated with insider threat detection, identification, assessment and management, (4) ensuring communication of insider risk activities and events among responsible participants in the Insider Risk Program, (5) providing governance and oversight of insider risk activities, and (6) integrating insider risk management with organizational or enterprise risk management generally.

Goal 1 - An Insider Risk policy exists.

The purpose of this goal is to ensure that the program has been established with the authority, scope, and responsibilities necessary to accomplish its mission.	Yes	Incomplete	No
1. Is there an authoritative document that establishes the existence of the Insider Risk Program?	☐	☐	☐
2. Does the authoritative document define the program's: - authority - scope - roles and responsibilities for stakeholders	☐	☐	☐

Goal 2 - There is detect, identify, assess, and manage capability for insider incidents.

The purpose of this goal is to ensure sufficient organizational capability exists to detect, identify, assess, and manage insider threats, in support of the Insider Risk Program.	Yes	Incomplete	No
1. Are the types of insider risks to be addressed identified and documented?	☐	☐	☐
2. Has a capability been established that supports detection, investigation, and response to insider risk types identified?	☐	☐	☐
3. Has a capability been established that supports prevention/ deterrence of insider risk types identified?	☐	☐	☐

Figure 2. Screenshot showing a portion of [CISA's Insider Threat Self-Assessment Tool](#).

Insider Threat Risk Management Principles and Best Practices

- Assumes that insider threat risk is always present – both "unintentional" and intentional insider threat actors.
- Access control and data handling measures serve to minimize insiders' unauthorized use of company assets and data.
- Engage a professional cybersecurity services firm to test networks specifically for insider threat exploits, and engage a third-party auditor to periodically review company logs and records for evidence of any anomalous behavior, such as moving assets, copying files, etc.
- Employ the "two-man rule" authorization to secure critical systems and assets.
- Promote a culture of reporting and train managers and employees to recognize the signs of potential indicators of insider threats.

Cyber Incident Response Plans and Drills. Cyber incident response plans are designed to provide businesses with a procedural road map of how to respond to a variety of cybersecurity incidents.[57] Although creating an incident response plan requires substantial amounts of time, resources, and planning,[58] having a well thought out plan on hand means the business knows exactly what to do to effectively respond in the midst of an emergent security incident and work toward restoring network operations to normalcy as quickly as possible. Cybersecurity incident response plans are a natural extension of business continuity, disaster recovery, and other contingency plans, with the objective being the rapid recovery and return to normal business operations.[59]

Even when a company develops a cybersecurity incident response plan, the plan is of little use unless employees are prepared and trained to implement the incident response as quickly as possible to contain the damage sustained by the incident. Similar to fire, natural disaster, active shooter, and severe weather drills, incident response drills provide response teams with the opportunity to practice how they should respond to a cyber security incident. Incident response drills, which can be tailored to practice responses to specific kinds of cybersecurity incidents (e.g., phishing attack, DoS attack, ransomware attack), can help incident response teams decrease their overall response and resolution times and prevent missteps in the execution of the incident response plan. Depending on a company's size, budget, and industry type, businesses can determine what cybersecurity incidents are best to prepare for, appropriate

[57] NIST SP 800-61, *Computer Security Incident Handling Guide*, Rev. 2 (August 2012), at 19 (hereinafter NIST Security Incident Handling Guide).
[58] Ibid., at 18.
[59] NIST, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 (Rev. 5 (2020), at 116.

scope and scale of incident response plans, and to what extent incident response teams may be wholly in-house, partially or entirely outsourced.[60]

Cyber Incident Response Plan and Drills: Principles and Best Practices
• Develop a cybersecurity incident response plan, using NIST guidelines. • Both NIST and CISA have multiple industry-specific resources for businesses. • Have mock incident response drills, which pressure-test and allow revisions to the plan. • Revisit and review the incident response plan on an annual basis, taking into account current trends in cybersecurity incidents and attacks and emergent risks (e.g., IoT and BYOD).

Who is Watching the Superusers? Irrespective of size, every company is likely to have one or more employees who have "superuser" access to the network. System and network administrators, who are responsible for managing other employees' access to company systems and network resources, are precisely the trusted insiders who could cause substantial damage if they abuse their access privileges and misuse company networks. In response to the infamous Edward Snowden case,[61] the National Security Agency rapidly accelerated its plan to accomplish a 90% reduction in its human system administrator workforce, from 1,000 to 100 individuals, in order to reduce the number of people who had superuser access to one or more systems within the NSA.[62]

Companies can also have their superuser employees sign an employment contract providing they would be liable for the misuse, abuse, or use of company systems, resources, or assets for improper purposes. Requiring these additional provisions in their employment

[60] *NIST Security Incident Handling Guide*, Note 57 supra, at 14.
[61] Edward Snowden was a government contractor who stole tens of thousands of classified documents from the NSA and posted them on the Internet, greatly damaging and compromising the United States' national security posture. A gifted systems administrator, Snowden was a superuser who was granted (and entrusted with) access to virtually the entire NSA. See, Greenberg, Andy. "After Six Years in Exile, Ed Snowden Explains Himself," (September 16, 2019), available at the Wired Magazine website.
[62] Davidson, Joe. "NSA to cut 90 percent of systems administrators," The Washington Post (August 13, 2013); Allen, Jonathan. "NSA to cut system administrators by 90 percent to limit data access," (August 8, 2013).

contracts also places superuser employees on notice of their greater responsibilities due to the special privileges the superuser role entails. Such superuser misconduct potentially carries civil and criminal penalties. Like all prospective and current employees, enhanced legal background checks showing arrests, charges, or convictions of crimes of dishonesty, fraud, or theft should be conducted on superuser employees. Companies should also require superuser employees, as a condition of continuing employment, to provide log activity summaries on a periodic basis and be audited by a professional, third-party audit services firm.[63]

Super Users – Principles and Best Practices
• Superusers are employees – usually system or network administrators - who have the highest privilege levels (and ability to access) company systems, networks, assets, and sensitive information or data, due to the nature of their role within the company. • Superusers should be advised up-front that, due to their role, they have special responsibilities and obligations to show they are performing their work in compliance with company policies and how these requirements are to be met (audits, log reviews, self-reporting of activities, etc.). • Consider adding terms to employment agreements to cover superusers' liability for privilege abuse and accessing company systems, resources, or assets for an improper purpose (or without a valid business purpose).

Creative Uses of Existing Tools to Enhance Locking Down and Deter Insider Threats. Companies of any size can leverage the tools they already have in creative and innovative ways to further lock down network systems and assets at little or no additional cost. For companies with additional resources and budget dollars to allocate for cybersecurity, additional practical measures can be implemented to provide additional protection against insider threats. Further, the creative use of the human factor can transform a company's workforce from being the weakest link to providing an additional layer of cybersecurity to its network.

[63] To require superuser employees to be subjected to a semi-annual or annual audit is no different than the standard practice of requiring a company's bookkeeper or accountant to be audited.

1. Best Cybersecurity Practices for Small Businesses

Many small businesses view themselves as lacking the human resources and budget needed to implement a robust cybersecurity program. Some small businesses perceive themselves as being too small to be the target of a cyberattack[64] or lacking the budgetary means to buy the latest state-of-the-art cybersecurity that would provide 100% protection against all cybersecurity threats. However, small businesses have increasingly become the targets of cyberattacks precisely because they are less likely to have adequate controls in place to either detect or mitigate the attack. Additionally, small businesses' increasing reliance on third-party software services delivered over the internet increases cybersecurity risk in three ways: (1) small businesses become vulnerable to interruptions in normal business operations if the third-party service provider experiences a cyber-attack or service failure impacting the delivery of its services to small business clients; (2) supply chain cyber-attacks are becoming increasingly common, which increases small business' risk to this kind of attack;[65] and (3) the small business' network becomes more complex in proportion to its reliance on third-party technologies, platforms, networks, and payment systems for normal day-to-day business operations.

In addition to the best cybersecurity practices applicable to all companies, small businesses can adopt the following low to no cost practices to minimize and prevent unauthorized access to company networks: (1) develop and cultivate a cybersecurity readiness work culture, with buy-in from the top down; (2) implement cybersecurity risk awareness training and best cyber hygiene practices for all employees; (3) keep sensitive company

[64] CISA Security Tip (ST06-002), *Debunking Some Common Cybersecurity Myths*, available at the CISA website.
[65] Although the bulk of the publicity and reporting on the 2020 Solar Winds cyberattack focused on the hackers' accessing to the networks of several federal agencies, this cyberattack equally impacted every business that had Solar Winds (and received security updates) on its network systems, including small business customers of Solar Winds. See, e.g., Toot, Kiersten, "4 Ways to Prevent a SolarWinds-Style Hack From Hitting Your Small Business," (December 24, 2020).

information (such as marketing strategies and trade secrets) segregated from the rest of the network or on a computer not connected to the rest of the company network; and (4) for employees working with customer data, provide specialized training on handling customer personal information.[66] Small companies can determine and prioritize what assets, systems, and information should be protected and then build their cybersecurity programs from that starting point[67] and also review recent changes to state consumer data protection and privacy laws which may impose additional requirements on businesses.[68]

Best Practices for Small Businesses
• Prioritize cybersecurity and get buy-in from top management down. • Leverage online resources (NIST and CISA[69] resources for Small Businesses) to create a cybersecurity program that is tailored to the specifics of the small business. • Implement access controls to right-size employee access to company systems and educate employees on the meaning and scope of authorized access. • Use Data Loss Prevention tools and develop data handling and disposal policies to prevent inadvertent or deliberate data exfiltration. • Provide continual cybersecurity training and awareness for employees at all levels (up to the CEO), emphasizing the importance of the Human Factor in cybersecurity risk management. • Promote a cybersecurity readiness work culture, including reporting of potential incidents and threats.

2. Best Cybersecurity Practices – Medium-Sized Company, Some Cyber/IT, Medium Budget

Medium-sized companies can implement all of the things discussed for small businesses, but should also look at the following:

[66] Interview, Justin Elze, *Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World*, 2019, Threatcare Press, at 140 ("The biggest myth about cybersecurity is that spending more money makes you more secure").
[67] Pinto, Ariel. "ODU Expert Offers Cybersecurity Tips for Small Businesses," (October 15, 2021).
[68] See, e.g., the Virginia Consumer Data Protection Act, Va. Code § 59.1-575 et seq.
[69] CISA Small Business Resources Publications Library (Cybersecurity); NIST Small Business Cybersecurity Corner.

Size and complexity of the network. Since medium-size companies are more likely to have multiple departments, in addition several classes (roles) of employees who have different access requirements. While the principle of least access still applies, not all employees would need to have the same access privileges to the same systems to perform their jobs. Additionally, selective (assets, resources, data) segregation and network segmentation protect company resources by limiting employees' access to only what is needed to do their jobs.

Use of Automation for Routine Network Administrative Tasks. Medium-sized companies should also consider automating system network administration to reduce the number of humans who have much higher access privileges than other employees to company networks. Automation also frees up network administrators to focus on higher priority work. Several vendors offer flexible network security management solutions on a subscription basis, which are scalable to meet a company's specific needs.[70]

Managed Service Providers to Manage Superusers. With more budgetary discretion and resources, medium-size companies may use managed service providers (MSP) to provide an automated network management solution, including monitoring, software, oversight, updates and reporting on company network systems. A managed service provider may also offer zero trust principles and architecture implementation solutions and support at affordable prices.

Vendor Services Contracts. Many medium-sized businesses should review and consider adding data protection and security provisions to vendor services contracts so the cybersecurity risks are appropriately shared between businesses and the vendors they utilize.

[70] See, e.g., Network Automation and Orchestration Tools Reviews and Ratings, Gartner Peer Insights.

CISA also provides ample resources for medium-size businesses for vendor cybersecurity risk management.[71]

Best Practices for Medium Sized Businesses
• Determine appropriate network and system segmentation, asset segregation, and access levels for all categories of employees at the company. • Segregate and segment out where assets and data reside on the network, paying close attention to who has access to which portions of the network – and whether access to one part of the network could inadvertently provide employees with access to other parts of the company's network. • Consider using automation and or Managed Service Providers (MSPs) to deliver an integrated cybersecurity solution, while freeing up resources to further develop cybersecurity policies, training and awareness, and incident response plans.

3. Best Cybersecurity Practices – Large Company, Large Cyber/IT, Large Budget

In addition to the best practices and recommendations for small and medium-sized businesses, large companies can do the following:

Service Provider Oversight, MSPs and Automated Solutions. A large company is likely to have several IT departments (or outsourced services) to provide company network management. Large companies which rely on vendors to provide services should have a system in place for overseeing and ensuring the vendors are not introducing cybersecurity risks into the company network or systems. While several MSPs (and other cybersecurity vendors) could provide cybersecurity services and support all divisions within a company, the company should also put other processes and controls into place to: (i) prevent over-reliance on vendor services, and (ii) provide the company with alternatives if any MSP or vendor ends up becoming a victim

[71] CISA, Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium-Sized Businesses, (September 2021).

of a cyberattack. Vendors should also agree to periodic audits and monitoring to ensure they employ best cybersecurity and cyber hygienic practices when delivering services, to minimize supply chain cybersecurity risks to the company. Consistent with business continuity, disaster recovery, and incident response plans, large companies should plan for failover and backup plans to mitigate the effects of supply chain cyberattacks, especially in cases where the vendor's services are essential to the company's business continuity and everyday functioning.

Creative Uses of the Human Factor to Augment Network and System Cybersecurity. Large companies have the budgetary means and resources to use creative tools to deter bad actors from accessing the network to misuse or steal assets or data. One reason why trusted insiders abuse and misuse their access is because they believe no one is watching – and in most cases, that is true. However, companies that require users to go through an extra layer of authentication – by having users contact a human person to be granted access to a critical resource, for example, – create a powerful psychological deterrent in doing so. By adding the human factor in as a guard rail, would-be bad actors are strongly deterred from misusing their access because, in this instance, there is someone watching. Similarly, the use of dual authorization (the "two-man rule") to access a critical system or sensitive area in the workplace minimizes insider threat risks because the two individuals would have to work in collusion in order to abuse access and misuse company information. In both cases, the human factor provides two things the bad actor does not want: (1) a track record; and (2) a witness. Similarly, time-sensitive controls which automatically log users' attempts to access systems or resources during off-hours also provide an effective deterrent, so long as the logs are reviewed in a timely fashion, or controls are set up to automatically send alerts to a human system administrator who can review the activity logs and determine whether the activity is suspicious, or not.

Best Practices for Large Businesses
• Formal vendor oversight, audits, and monitoring, to ensure vendors are not creating additional cybersecurity risks for the company. • Business continuity and disaster recovery plans should include failover plans so the company can easily pivot if an MSP or vendor sustains a cyberattack, or other impacting event. • Add psychological deterrents – actual humans – to augment access control measures at off hours, or to critical systems. • Depending on the department, lock down files, folders, and drives using time-sensitive parameters to govern employee access – and make employees aware of the special access control measures in place for specific assets (sensitive information, personal data, etc.).

IV. Conclusion

Reports of cybersecurity incidents resulting from trusted insiders' misconduct are increasing. The Supreme Court decision to narrow the meaning of "unauthorized access" in *Van Buren* has the unfortunate effect of placing the onus on businesses to implement more stringent access control and network monitoring measures to protect against insider threats. Although the Supreme Court's interpretation of the term "exceeds unauthorized access" seems counterintuitive, its intent was to err in the direction of avoiding overcriminalization and the arbitrary application of the CFAA to innocuous, ordinary computer use by millions of employees in the workplace. Until Congress acts to clarify the language of the CFAA, employers cannot rely on the CFAA to hold employees liable for misuse or abuse of their access to assets on company networks. Companies should take the time, irrespective of their size or budget, to determine what cybersecurity measures should be adopted to minimize insider threats and attacks from outside hackers. Given the amount of low to no-cost resources available to help companies determine what cybersecurity solutions would work best for them, irrespective of their size, industry, and other contextual factors, businesses should prioritize their time and resources to do everything they can to protect users and assets on company networks.