



USING THE POWER OF THE WORKFORCE TO DRIVE CYBERSECURITY OBJECTIVES

EDITED BY DR. EDWARD AMOROSO
CEO & SENIOR ANALYST, TAG CYBER

USING THE POWER OF THE WORKFORCE TO DRIVE CYBERSECURITY OBJECTIVES

EDITED BY DR. EDWARD AMOROSO,
CEO & SENIOR ANALYST, TAG CYBER

*This ebook examines how positive influences on employee behavior can improve cyber risk posture. The chapters discuss how technology can be used to guide improved decision making through empowerment, as opposed to more traditional bounds on user behavior that often reduce productivity and employee experience. The commercial **Nudge Security** platform is used to demonstrate this approach in a practical enterprise setting.*

INTRODUCTION

CAN EMPLOYEES MAKE BETTER SECURITY DECISIONS?

Page 3

CHAPTER 1

HOW USER DISCRETION INFLUENCES SECURITY

Page 4

CHAPTER 2

HOW TECHNOLOGY CAN BE USED TO GUIDE SECURITY DECISIONS

Page 7

CHAPTER 3

THE IMPACT OF EMPLOYEE DECISIONS ON CYBER RISK

Page 9

CHAPTER 4

HOW SAAS SUPPLY CHAIN RISK IS AFFECTED BY USER DECISIONS

Page 11

CHAPTER 5

AN ACTION PLAN TO IMPROVE WORKPLACE SECURITY DECISIONS

Page 13

CAN EMPLOYEES MAKE BETTER SECURITY DECISIONS?

DR. EDWARD AMOROSO, CEO, TAG CYBER

Employee decisions significantly affect cybersecurity posture. An important question for enterprise teams is whether such decision making can be “nudged” in the right direction.

As security threats grow, employees can—and should—improve their decisions regarding cybersecurity. For example, important data is frequently lost through the improper sharing of email file attachments. Similarly, sensitive data is often leaked, because it is poorly marked by owners, thus allowing it to slip past data-leakage protection defenses. As a result, security awareness has become an important aspect of most enterprise security programs.

Not everything can be blamed, however, on the poor judgment of employees. In some cases, security risks stem from the difficult circumstances in which employees operate. For instance, employees who deal with complex workflow activity, or are tasked with handling complicated business interactions, can be quite vulnerable to data mishandling, even if they are experienced and well trained in cybersecurity.

As a result, new approaches are required to help employees make good decisions, outside the standard assumptions that training programs will work or that penalizing errors will decrease the rate of data loss. Much more creative and supportive strategies are needed, including ones based on advanced technology. Enterprise security teams would be wise to consider how they can employ such means to reduce risk.

In this five-chapter ebook, members of the **TAG Cyber** analyst team outline this general challenge, as well as review whether employees and third parties can be guided in the right direction through a combination of technology and engagement.

HOW USER DISCRETION INFLUENCES SECURITY

DR. EDWARD AMOROSO, CEO, TAG CYBER

The interplay between the mandatory controls set up by administrators and the discretionary controls managed by individual users represents the underlying playing field for security teams to drive better decision making.

Understanding how employee decisions affect cybersecurity posture is a critical first step in establishing a technology-based program that leads toward making better choices.

The original framers of computer security grappled with how to ensure that data and systems had proper controls. In the 1980s, for example, the U.S. government developed a framework called the **Orange Book**, which pioneered the use of security requirements to measure how well control deployment was done. Several ideas that originated in this early work continue to guide many operating principles used today, including how employees are expected to make security decisions.

Mandatory and Discretionary Controls

Two types of security controls can be deployed to any computing environment. The first involves mandatory controls, which do not rely on users to make decisions. Mandatory controls are, instead, configured by security teams and IT administrators. For example, in this case, users do not have to make many decisions about whether to use two-factor authentication (2FA); this decision is appropriately made for them. While mandatory controls may be implemented in the context of a corporate network login, domain account or single sign-on (SSO) environment, it can be a challenge in other environments. For example, some SaaS implementations could include controls that are designed specifically to empower each user to manage their controls, such as whether to deploy multifactor authentication.

The second type involves discretionary controls, which provide leeway in how—or even whether—they are used. Such controls do rely on the judgment and decision making of users for security. For example, filesharing is often implemented without much mandatory control on how access is managed, whether encryption is used, or what types of data are included. If a user makes a bad decision, this can have a negative impact.

Administering Mandatory Controls

Despite the fact that mandatory controls do not allow users to make decisions, their setup and administration do require good judgment from

administrators. As such, the humans involved in the design, implementation and operation of these controls must also make good decisions for policy enforcement. The ability to influence these decision makers is thus a key requirement for the correct implementation of mandatory controls.

This is a profound issue for cybersecurity, because it underscores the fact that such a significant portion of any given control's effectiveness truly depends on the good decisions and choices made by individual humans. This risk is usually attributed to normal users, but it should be obvious that system and security administrators who possess the highest levels of privileged access will have an even greater impact on cyber risk profiles.

Implementing Discretionary Controls

The use of discretionary controls obviously demands that assistance or support be provided to guide and influence good judgment and decision making by users, and two options are available. The familiar option is to provide extensive training and awareness for employees in the form of videos, courses and other artifacts. This approach should be well known to anyone who works in a company—and is a recommended practice in every environment.

The second option involves the use of technology to guide user decision making. When technology is used, the platform can tailor training and guide the situation. For example, developers could be nudged to make one type of security decision related to their work (e.g., DevOps, CI/CD pipelines), whereas business managers might be trained to make another type of decision related to their type of work (e.g., budget planning, finance).

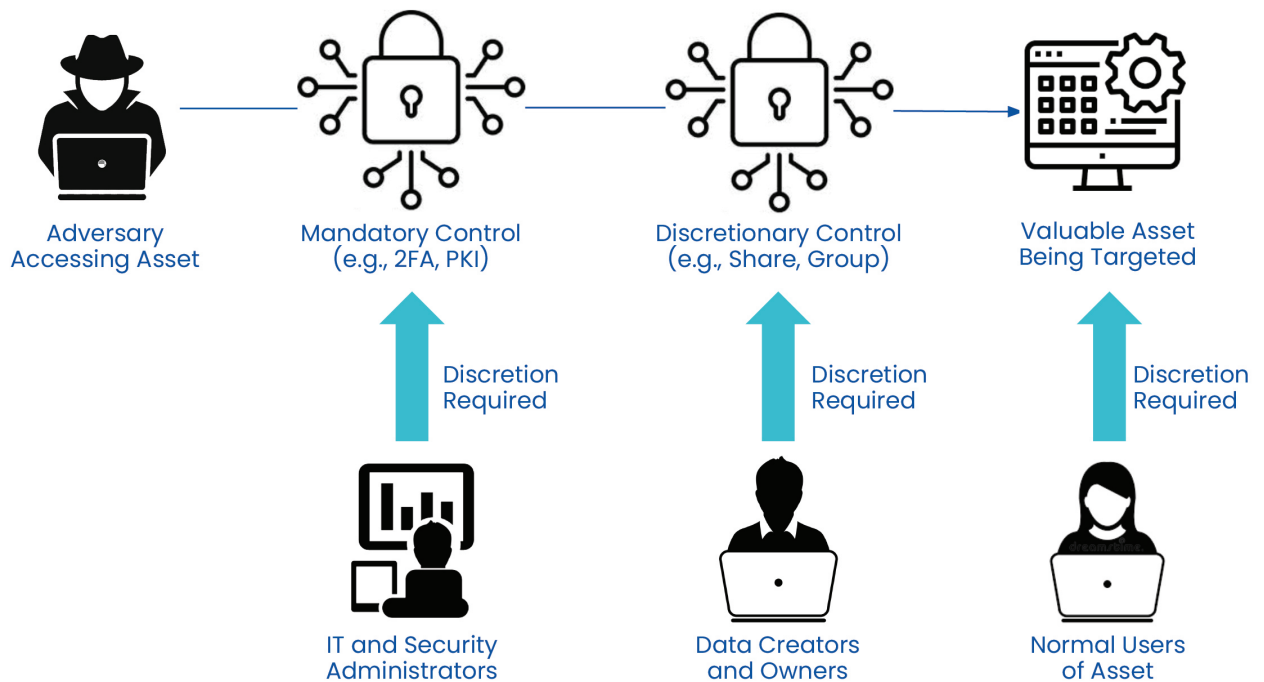


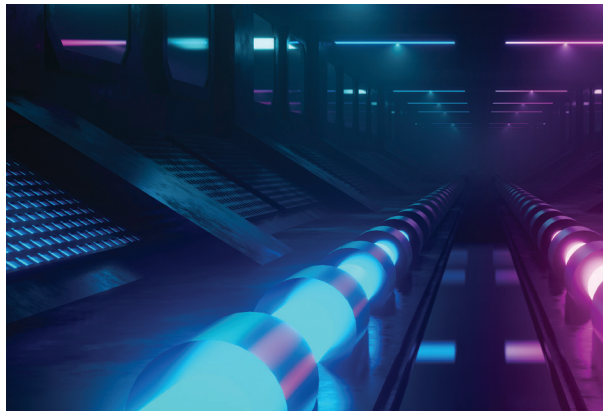
Figure 1.1 Mandatory and Discretionary Controls

As depicted in Figure 1.1, the interplay between the mandatory controls set up by administrators and the discretionary controls managed by individual users represents the underlying playing field for security teams to drive better decision making. As one would expect, the use of technology platforms to govern the rules of this playing field has many advantages, including the ability to scale across a large enterprise environment.

Nudge Technology

The commercial **Nudge Security** platform focuses on using technology to guide all types of users through the decision-making process when accessing tools, systems and data. As suggested above, this approach allows for a better tailored response to the situation, and, of course, can be deployed in conjunction with a number of other security controls and processes. Technology and training are compatible and can be operated in parallel.

Enterprise teams are strongly encouraged to review their technology options for guiding discretion by users, developers, administrators and other individuals in security-related decision making. The Nudge Security approach is promising in this regard, especially for highly distributed organizations trying to maintain visibility and governance of discretionary controls in the context of their evolving infrastructure.



HOW TECHNOLOGY CAN BE USED TO GUIDE SECURITY DECISIONS

DR. EDWARD AMOROSO, CEO, TAG CYBER

For many years, cybersecurity solutions focused on preventing bad things from happening. More modern solutions have found that shifting the emphasis toward enabling good things to happen can achieve better results.

Advanced technology-based solutions can offer a practical solution to the challenge of optimizing security decision making by employees.

Nudge Security emerged in October 2022 after a period of stealth development under the direction of co-founders Jaime Blasco and Russ Spitler, former technology leaders at **AT&T Alien Labs**. Seed funding for the company was provided by **Ballistic Ventures**, comprised of an iconic group of cybersecurity luminaries, including Roger Thornton, Barmak Meftah, Jake Seid, Ted Schlein and Kevin Mandia.

The basic concept driving the Nudge Security offering is that employee behavior can be influenced toward improved security decision making through the use of a supportive technology platform. When designing the platform, one of the main goals was to ensure the non-disruption of worker productivity by focusing on empowerment rather than the usual security approach of blocking, denying and mitigating user requests.

Using Nudge Security to Empower the Workforce

For many years, cybersecurity solutions focused on preventing bad things from happening. More modern solutions have found that shifting the emphasis toward *enabling* good things to happen can achieve better results. This idea of empowering users—including employees, contractors and third parties—to make good decisions is the fundamental basis for the Nudge Security platform. The insight that drives the Nudge Security solution is that, as employees interact with cloud and SaaS services, their decisions can be carefully (and properly) monitored to determine whether risk is being introduced inappropriately. **By ingesting such data and communicating with the user in a non-intrusive manner, the overall decision-making process can be guided toward meaningful improvement.**

Nudge Security's Platform-Assisted Security Architecture

The general platform operation for Nudge Security is depicted in Figure 2.1 below. The primary actors in its protection ecosystem are the employees—employed staff, consultants and other individuals with direct access to corporate resources—and the administrators of the Nudge Security platform (which is also presumed to be done by employees or other empowered staff with privileged access).

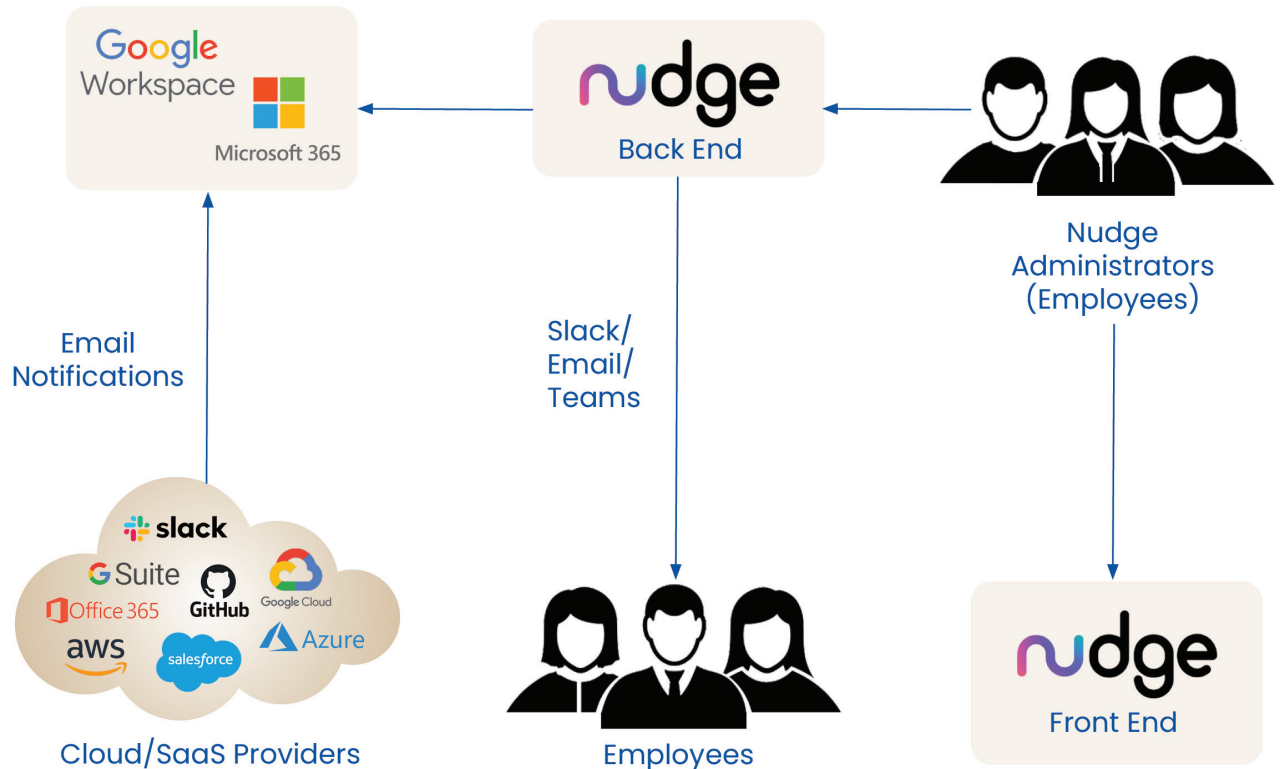


Figure 2.1. Nudge Security Architecture

The operation is straightforward: As employees interact with cloud and SaaS services—such as AWS, Office 365, Salesforce, Azure, Github, Google Workspace, Slack and Google Cloud—email notifications are regularly woven into their workflow. The Nudge Security platform ingests employee engagement and response safely, using this as the basis for guiding behavior.

A front-end dashboard is available to both employees and administrators to configure settings and manage accounts. A back-end system, which is accessible by administrators, generates email messages to employees to provide the recommended guidance, training or other information based on observed user behavior, thereby allowing employees to gain valuable insights into their decisions—and, consequently, develop better habits.

THE IMPACT OF EMPLOYEE DECISIONS ON CYBER RISK

JOHN J. MASSERINI, SENIOR ANALYST, TAG CYBER

Today's astute workforce has platforms at their disposal that solve almost every conceivable problem, fundamentally transforming how companies look at risk.

With more access to technology and systems than ever before, it is essential that employees make informed cybersecurity decisions.

While most organizations would admit that “shadow IT” was a rising concern pre-pandemic, many employers turned a blind eye during the two-plus years of work from home, significantly exacerbating the issue. The challenge of undersized VPNs, outdated authentication practices, and the general inconvenience of long-term remote access prompted employees to find whatever workaround they could, simply to make their day-to-day life easier. Now with all these employees returning to the office, the services and functionality they grew accustomed to are also coming into the infrastructure. The dual challenge of that movement involves integrating their known required services—such as Zoom and Microsoft Teams—into the infrastructure, and, secondly, trying to determine what additional unknown services are being used.

The crux of the issue boils down to the risk of employees storing sensitive information—be it business plans, marketing strategies, credit card data, or customer and patient records—in an unsecured third-party environment. Historically, policies prevented using such solutions, resulting in security teams attempting to use web gateways or proxies to limit employee access to these services, with only moderate success.

While these employees could be chastised for violating the policies they should have known, the fact is, they were simply making decisions based on the inadequacy of what they were given to work with. Technology that was implemented to be used within the corporate network was suddenly inadequate when employees were flung far and wide. However, deadlines were still in place and deliverables had to be dispatched, leaving employees no other choice than to leverage external services.

As all these employees come back to the office, they are bringing their Smartsheets, LucidCharts, Jira and Zapier functionality with them, as if

these solutions belonged there. Discord chats are resolving production issues, WeTransfer is delivering marketing content to third parties, and DropBox has a year's worth of sales and client reports.

Security teams tend to think of risk first and are too often quick to blame users for not doing what they are "supposed" to be doing. However, when the average user needs to choose between meeting a deadline, making their boss happy, or following security protocol, they will almost always choose the first option. After all, performance reviews are evaluated by on-time deliverables, revenue generation and customer satisfaction—but, usually not on adherence to security processes. No one should be surprised when employees make decisions based on productivity rather than risk.

Interestingly, while many organizations are now adopting these previously forbidden services, they continue to struggle with moving their employee base from insecure versions to approved ones. The primary reasons for employee reluctance are twofold: they are comfortable with what they have, and they don't know how to register for or use the new service.

The bottom line is that employee decisions are a huge piece of the cybersecurity puzzle, and the curation and guidance of these decisions must be closely considered.



HOW SaaS SUPPLY CHAIN RISK IS AFFECTED BY USER DECISIONS

CHRISTOPHER R. WILDER, TAG CYBER

When organizations choose SaaS from sources that haven't been vetted by cybersecurity experts, they open themselves to potential security vulnerabilities.

When poor cybersecurity decisions are made by employees or third-party suppliers and partners, the negative impact on the enterprise supply chain can be significant.

Software as a Service (SaaS) applications have become increasingly popular in the corporate world, providing organizations with easy access to the tools and capabilities essential to their business. However, as with any third-party software, SaaS introduces new elements of risk into an organization. When employees, third-party suppliers and partners make poor cybersecurity decisions, the negative impact on the enterprise supply chain can cause significant damage.

Bad Decisions Cause Bad Outcomes

One key area where poor decision making increases SaaS supply chain risk is the selection and implementation of SaaS. When organizations choose SaaS from sources that haven't been vetted by cybersecurity experts, they open themselves to potential security vulnerabilities. Too much reliance on these providers increases the risk of system downtime or data breaches, while improperly integrated SaaS applications and processes create new entry points for cyberattacks.

To mitigate supply chain risks, it is essential for organizations to carefully vet and select SaaS providers to ensure that the SaaS solution is properly integrated and maintained, including conducting thorough due diligence on the SaaS provider, understanding the provider's security protocols, and implementing strict protocols for testing and deploying new software.

In addition, as IT and SaaS procurement has become more decentralized across business departments and individual users, the related processes of third-party risk management and SaaS vendor security assessment have also become much more difficult.

Reducing SaaS Supply Chain Vulnerabilities is Imperative

One tool that organizations can use to reduce the risk of SaaS supply chain vulnerabilities and booster third-party risk management is **Nudge Security**. Most importantly, the product helps organizations manage and improve their cybersecurity practices related to SaaS applications by providing a comprehensive view of an organization's cybersecurity posture, including the security practices of its SaaS providers. Nudge also enables organizations to identify potential vulnerabilities, vastly simplifying the process for vendor security assessments. Additionally, Nudge Security helps employees make secure choices with timely "security nudges," which offer helpful guidance as they adopt and use SaaS. Some of these "nudges" include updating passwords when necessary, suggesting approved alternative applications, and turning on MFA when disabled.

Organizations use Nudge Security for several use cases, including:

- **Supply Chain Visibility.** A manufacturing company using the Nudge platform can monitor SaaS providers and analyze their security posture, helping them identify and mitigate the risk of supply chain vulnerabilities. This company will have a comprehensive view of the overall security posture of their SaaS providers, which can help them make informed decisions about the security of their overall digital supply chain.
- **Preventing Phishing Campaigns.** A software company using Nudge Security can inventory every cloud and SaaS asset created in the organization in order to seamlessly track and categorize assets within the scope of SOC 2 certification. The company can then run a playbook to automate the SOC 2 access review process, ensuring that SaaS accounts are deprovisioned quickly and completely for offboarded employees.
- **Compliance Monitoring.** A financial service company using Nudge Security can monitor the compliance of their SaaS providers, especially for regulations such as PII, HIPAA, CMMC or GDPR, thereby supporting their efforts to protect customer data and meet industry standards.

How Nudge Security Helps Organizations Protect Their SaaS Supply Chain

By using a tool like Nudge Security to take the above steps, organizations can proactively manage SaaS supply chain risk by ensuring they take all the necessary precautions to protect themselves and their customers from cyberthreats. Nudge Security not only helps organizations avoid costly disruptions and data breaches, but it also improves customer trust and confidence in the organization's security practices. Organizations can maintain the trust of their customers and stakeholders by guaranteeing continuous, smooth business operations, while complying with industry regulations and standards.

AN ACTION PLAN TO IMPROVE WORKFORCE SECURITY DECISIONS

DR. EDWARD AMOROSO, CEO, TAG CYBER

The TAG Cyber team recommends the Nudge Security solution be included in the source selection process, since the solution includes many desirable attributes, as described in this ebook.

Enterprise teams should implement an action plan to help guide employees toward making better cybersecurity decisions in their day-to-day work.

Enterprise security teams will benefit from reviewing their existing approach to supporting, guiding and training workforce teams on security decision making. Most companies may find they have implemented a security awareness program with phish testing, but often little more. While every organization has a different baseline posture, the following steps will generally apply to improve workforce security decisions.

Step 1: Review Workforce Security Posture

Any plan for improving the security of workforce decision making must start with a posture assessment of existing strengths and weaknesses. The security team should review whether significant incidents have occurred (or been avoided) as a result of employee behavior. Existing awareness, training and user testing should also be identified and documented.

Step 2: Define Objectives for Workforce Security Decision Making

The security team is advised to identify reasonable improvement objectives for workforce security decision making. This can be done informally as a series of stated goals, or it can be embedded into a more formal quantitative risk objective, usually expressed in a “from-to” statement where an existing level of unacceptable organizational cyber risk is reduced to a more acceptable level.

Step 3: Review Available Platform Solutions

Since effective automated platforms currently exist that can guide the workforce toward improved security decision making, security teams are advised to spend time in commercial source selection to review platform options. As one would expect, the TAG Cyber team recommends the Nudge Security solution be included in the source selection process, since the solution includes many desirable attributes, as described in this ebook.

Step 4: Integrate the Selected Platform into Workflows

The final step is to plan the integration of the selected workforce security platform into suitable and applicable business workflows. This is likely best done with the assistance of the vendor, especially since this capability is new and few security teams will have the experience applicable to this type of control. As always, the TAG Cyber analysts are available to assist enterprise teams with this process.

Step 5: Measure Progress Against Defined Objectives

Once the Nudge Security platform is in place across the enterprise, its protection benefits to the organization should begin to emerge. Obviously, the main objective is not to merely get the platform deployed, but to use the automation and platform features to engage, empower and guide employees toward proper security decision making. Once in place, cyber risks should begin to wane as employee-related incidents reduce in frequency and intensity.



ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective..

ABOUT NUDGE

Nudge Security's mission is to secure modern organizations through the power of the modern workforce. Founded in 2021 by Jaime Blasco and Russell Spitler, Nudge Security's technology solutions help distributed, high-growth organizations improve cybersecurity postures by engaging workers in smart security decision making. The early-stage startup is funded by Ballistic Ventures

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso, John J. Masserini, Christopher R. Wilder

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non- analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by Nudge Security, Inc. TAG Cyber provides research, analysis and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. TAG Cyber disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of TAG Cyber's analysts and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

TAG Cyber may provide forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment and opinion on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially.

You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.

Copyright © 2023 TAG Cyber LLC. This report may not be reproduced, distributed or shared without TAG Cyber's written permission. The material in this report is composed of the opinions of the TAG Cyber analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy or completeness of this report are disclaimed herein.