Sarbanes Oxley Compliance Professionals Association (SOXCPA)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.sarbanes-oxley-association.com

Sarbanes Oxley News, April 2023

Dear members and friends,

According to the PCAOB, the modernization of standards addressing core auditing principles and responsibilities is necessary.

Advancing the Board's strategic goal of modernizing PCAOB standards, the proposal would replace a foundational group of standards that have not changed significantly since their adoption on an interim basis in 2003.

The Public Company Accounting Oversight Board (PCAOB) issued for public comment a proposed new standard, AS 1000, General Responsibilities of the Auditor in Conducting an Audit. The Board requests public comment on the proposal by May 30, 2023.

If adopted, AS 1000 would reorganize and consolidate a group of standards that were adopted on an interim basis by the PCAOB in April 2003 and that address the core principles and responsibilities of the auditor, such as reasonable assurance, professional judgment, due professional care, and professional skepticism.

The proposal would also amend certain other standards that address responsibilities fundamental to the conduct of an audit.

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

Proposed Auditing Standard – General Responsibilities of the Auditor in Conducting an Audit
and
Proposed Amendments to PCAOB Standards

PCAOB Release No. 2023-001
March 28, 2023

PCAOB Rulemaking
Docket Matter No. 049

Among other changes, the amendments would:

(1) reinforce and clarify the engagement partner's responsibility to exercise due professional care related to supervision and review, and

(2) accelerate the documentation completion date by reducing the maximum period for the auditor to assemble a complete and final set of audit documentation from 45 days to 14 days.

"Our capital markets never stop evolving, and PCAOB standards must keep up to keep investors protected," said PCAOB Chair Erica Y. Williams. "This proposal would modernize standards that are foundational to audit quality, ensuring they are fit to meet today's challenges."

Since the PCAOB's adoption of the interim standards in 2003, the auditing environment has continued to develop in many ways, including new PCAOB standards, new or revised independence requirements, and advancements in technology affecting the availability of electronic audit evidence and use of audit software.

The proposal would bring important improvements designed to reflect changes in the auditing environment, eliminate outdated and inconsistent language, and increase consistency throughout PCAOB standards.

Detailed questions are included throughout the proposal, and commenters are encouraged to:

(1) comment on any or all topics,

(2) respond to any or all questions,

(3) provide feedback in areas not covered by specific questions, and

(4) provide any evidence that informs commenters' views.

Executive summary

We are proposing a new auditing standard, AS 1000, General Responsibilities of the Auditor in Conducting an Audit ("proposed standard" or "proposed AS 1000").

Proposed AS 1000 would replace a group of standards originally developed by the American Institute of Certified Public Accountants ("AICPA") and adopted on an interim basis by the PCAOB in 2003.

That group of standards establishes the general principles and responsibilities of the auditor when conducting an audit ("foundational standards").

The general principles and responsibilities addressed by the foundational standards include reasonable assurance, due professional care, professional skepticism, independence, competence, and professional judgment.

These principles and related responsibilities provide a foundation for the proper performance of the audit.

Through this standard-setting project, we are reaffirming the general principles and responsibilities to ensure that the foundation continues to be solid and appropriate for maintaining high-quality audits.

These principles and responsibilities, together with modernized auditing standards, should equip the auditor with better tools to protect investors and further the public interest in the preparation of informative, accurate, and independent audit reports.

Currently, the general principles and responsibilities are addressed across four standards: AS 1001, Responsibilities and Functions of the Independent Auditor; AS 1005, Independence; AS 1010, Training and Proficiency of the Independent Auditor; and AS 1015, Due Professional Care in the Performance of Work.

The proposal would combine the general principles and responsibilities from these standards into one standard (proposed AS 1000), while also making updates to reflect developments in the auditing environment.

We are also proposing to amend certain other standards that address responsibilities fundamental to the conduct of an audit.

These amendments would clarify the engagement partner's responsibility to exercise due professional care related to supervision and review of the audit, accelerate the documentation completion date by reducing the maximum period for the auditor to assemble a complete and final set of audit documentation from 45 days to 14 days, and clarify the auditor's responsibility to evaluate whether the financial statements are "presented fairly."

Finally, we are proposing additional amendments to conform to these changes.

To read more: https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-proposes-modernization-of-standards-addressing-core-auditing-principles-and-responsibilities

2023 Inspections to Prioritize Audit Risks Related to Fraud, the Financial Services Sector, Crypto

The Public Company Accounting Oversight Board (PCAOB) inspectors outlined their priorities for 2023 inspections in a new PCAOB staff report.

The report outlines plans to increase the focus on fraud-related audit procedures, continue prioritizing risks related to material digital assets, and continue selecting audits in the financial services sector for inspection, among other priorities.

SPOTLIGHT

Staff Priorities for 2023 Inspections

"Increased deficiencies in 2021 inspections and increased comment forms in 2022 inspections revealed a troubling trend in audit quality, which we are tackling head-on in 2023," said PCAOB Chair Erica Y. Williams. "By staying ahead of new and emerging risks, our inspections plan will hold firms accountable and drive improvements in audit quality for investors."

Last year, the PCAOB found a year-over-year increase in the number of audits with deficiencies at audit firms that the PCAOB inspected in 2021. Chair Williams said higher deficiency rates in 2021, coupled with increased comment forms for 2022, were a warning signal. She challenged the audit profession to sharpen its focus on improving audit quality and protecting investors.

The complete list of 2023 inspection priorities outlined in today's report includes:

1. Risk of fraud
2. Auditing and accounting risks
3. Risk assessment and internal controls
4. Financial services specific considerations
5. Broker-dealer specific considerations
6. M&A, including de-SPAC transactions
7. Digital assets
8. Use of the work of other auditors
9. Quality control (particularly talent retention and its impact on audit quality, and independence)

10. Other areas of inspection (critical audit matters, cybersecurity, and use of data and technology in the audit)

The report notes the target team of inspectors, who execute in-depth reviews across audit firms each year, will focus its work in 2023 on audits that include risks related to digital assets, first year audits, multi-location audits, and significant or unusual events or transactions.

As part of ongoing efforts to enhance inspections, today's report also says inspectors will expand the number of audits they review for certain annual firms.

Financial Reporting and Audit Risks

The existence of the following factors may increase the risk of inaccurate, incomplete, or untimely financial information and may have required changes to the audit procedures:

- Unreasonable assumptions and models used to value complex financial instruments and accounting estimates (e.g., derivatives).
- Increased volatility in financial and commodity markets due to fluctuations in interest rates and inflationary trends.
- Unreasonable assumptions in future financial projections used to account for estimates in business combinations; asset impairment; impairment of goodwill and intangible assets; loss contingencies and valuation allowances; and revenue.
- Unreasonable assumptions affecting the timing and amount of revenue recognition due to supply chain disruptions, negative effects of COVID-19, and geopolitical conflicts.
- Complexities regarding existence and valuation of inventory, due to challenges with inventory build-up and obsolescence.
- Challenges with accounting for foreign currency and the effects of foreign currency transaction and translation adjustments on the financial statements, including the statement of cash flows, due to the rising value of the U.S. dollar at public companies with significant foreign operations.
- Financial, economic, and business uncertainties that impact the auditor's evaluation of the public company's ability to continue as a going concern, such as the public company's inability to access funds through borrowings due to violation of debt covenants or deal cancellations.
- Economic conditions that could adversely affect a public company's ability to meet certain criteria and/or assumptions, such as whether or not a public company has the ability and intent to not sell investment securities it has designated as "held-to-maturity."
- Complexities in the public company's activities that may impact disclosures regarding (1) contingent liabilities, (2) changes in classification of financial instruments between level 2 and level 3, (3) concentrations of credit risk, and (4) related party transactions that may result in omitted, incomplete, or inaccurate disclosures.

Reminders for Auditors

1. Understand the business of the public company or broker-dealer and its environment to understand the events, conditions, and activities that might reasonably be expected to have a significant effect on the risks of material misstatement.
2. Understand the potential for material misstatement due to fraud.
3. Focus on the basics of audit work such as performing core procedures like evaluating information for reliability.
4. When using information produced by a public company or broker-dealer as audit evidence, evaluate whether the information is sufficient and appropriate for purposes of the audit by performing procedures to (1) test the accuracy and completeness of the information or test the controls over the accuracy and completeness of that information and (2) evaluate whether the information is sufficiently precise and detailed for purposes of the audit.
5. Exercise professional skepticism, an attitude that includes a questioning mind, when gathering and objectively evaluating audit evidence.
6. Consider the impact of economic sanctions on financial reporting and compliance with laws and regulations.
7. Consider whether a cybersecurity-related incident impacting financial reporting occurred at the public company or broker-dealer that may require modification to the planned audit approach.
8. Perform procedures for the purpose of ascertaining the occurrence of subsequent events that may require adjustment to or disclosure in the financial statements (e.g., subsequent events that may affect realization of assets or the settlement of estimated liabilities that may require adjustment and/disclosure in the financial statements).

To read more: https://pcaobus.org/news-events/news-releases/news-release-detail/2023-inspections-to-prioritize-audit-risks-related-to-fraud-the-financial-services-sector-crypto
https://assets.pcaobus.org/pcaob-dev/docs/default-source/documents/priorities-spotlight.pdf?sfvrsn=5c104095_2

Consumer Compliance Supervisory Highlights

Federal Deposit Insurance Corporation

FEDERAL DEPOSIT INSURANCE CORPORATION

This issue of the FDIC Consumer Compliance Supervisory Highlights includes:

• A summary of the overall results of the FDIC's consumer compliance examinations of supervised institutions in 2022;

• A description of the most frequently cited violations and other consumer compliance examination observations;

• Information on examination observations and regulatory developments;

• A summary of consumer compliance resources and information available to financial institutions; and

• An overview of trends in consumer complaints that were processed by the FDIC in 2022.

Summary of Overall Consumer Compliance Performance in 2022

The FDIC supervises approximately 3,000 state-chartered banks and thrifts that are not members of the Federal Reserve System (supervised institutions). Most of these institutions are community banks that provide credit and services locally.

The FDIC, through its Division of Depositor and Consumer Protection (DCP), is responsible for evaluating supervised institutions for compliance with consumer protection, antidiscrimination, and community reinvestment laws.

The FDIC's consumer compliance examination program focuses on identifying, addressing, and mitigating the greatest potential risks to consumers, based on the business model and products offered by a particular institution.

The FDIC conducts periodic risk-based examinations of supervised institutions for compliance with over 30 Federal consumer protection laws and regulations. In 2022, the FDIC conducted approximately 1,000 consumer compliance examinations.

Overall, supervised institutions demonstrated effective management of their consumer compliance responsibilities.

The FDIC uses the Federal Financial Institutions Examination Council's (FFIEC) Uniform Interagency Consumer Compliance Rating System to evaluate supervised institutions' adherence to consumer protection laws and regulations.

As of December 31, 2022, 99 percent of all FDIC-supervised institutions were rated satisfactory or better for consumer compliance (i.e., ratings of "1" or "2"), as well as for the Community Reinvestment Act (CRA) (i.e., CRA ratings of "Outstanding" or "Satisfactory").

Institutions rated less than satisfactory for consumer compliance (i.e., ratings of "3," "4," or "5") had overall compliance management system (CMS) weaknesses, which often resulted in violations of law and the risk of consumer harm.

Institutions rated "needs to improve" or "substantial noncompliance" for CRA represent a weak performance under the lending, investment and service tests, the community development test, the small bank performance standards, or an approved strategic plan, as applicable.

Consumer Compliance Supervisory HIGHLIGHTS

Federal Deposit Insurance Corporation

Introduction 1

Summary of Overall Consumer Compliance Performance in 2022 2

Most Frequently Cited Violations 3

Consumer Compliance Examination Observations 5

Real Estate Settlement Procedures Act Section 8: Referral Arrangements 5

Fair Credit Reporting Act: Trigger Leads 6

Servicemembers Civil Relief Act: Automatically Applying Excess Interest Payments to Principal Loan Balance 7

Fair Lending 8

Regulatory and Other Developments 10

PAVE Task Force 10

Community Reinvestment Act Rulemaking 10

Special Purpose Credit Programs under ECOA 11

Home Mortgage Disclosure Act – Threshold Changes 11

Flood Insurance: Revised Interagency Questions and Answers 12

Final Rule Relating to False Advertising, Misrepresentations About Insured Status, and Misuse of the FDIC's Name or Logo 12

Notice of Proposed Rulemaking Relating to FDIC Official Sign and Advertising Requirements, False Advertising, Misrepresentations of Insured Status, and Misuse of the FDIC's Name or Logo 12

Notification of Engaging in Crypto-Related Activities 13

Amendments to Guidelines for Appeals of Material Supervisory Determinations 14

Supervisory Guidance on Multiple Re-Presentment NSF Fees 14

Resources for Financial Institutions 15

Banker Resource Center 15

An Overview of Consumer Complaint Trends 16

To read more: https://www.fdic.gov/regulations/examinations/consumer-compliance-supervisory-highlights/documents/ccs-highlights-march2023.pdf

SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

The Securities and Exchange Commission proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.

"Over the years, our disclosure regime has evolved to reflect evolving risks and investor needs," said SEC Chair Gary Gensler.

"Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks. A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner. I am pleased to support this proposal because, if adopted, it would strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting."

The proposed amendments would require, among other things, current reporting about material cybersecurity incidents and periodic reporting to provide updates about previously reported cybersecurity incidents.

The proposal also would require periodic reporting about a registrant's policies and procedures to identify and manage cybersecurity risks; the registrant's board of directors' oversight of cybersecurity risk; and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures.

The proposal further would require annual reporting or certain proxy disclosure about the board of directors' cybersecurity expertise, if any.

The proposed amendments are intended to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification to investors of material cybersecurity incidents.

The proposing release will be published on SEC.gov and in the Federal Register.

The comment period will remain open for 60 days following publication of the proposing release on the SEC's website or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.

To read more: https://www.sec.gov/news/press-release/2022-39

https://www.sec.gov/rules/proposed/2022/33-11038.pdf

A. Overview 18

B. Reporting of Cybersecurity Incidents on Form 8-K 20

1. Overview of Proposed Item 1.05 of Form 8-K 20

2. Examples of Cybersecurity Incidents that May Require Disclosure Pursuant to Proposed Item 1.05 of Form 8-K 24

3. Ongoing Investigations Regarding Cybersecurity Incidents 25

4. Proposed Amendment to Form 6-K 26

5. Proposed Amendments to the Eligibility Provisions of Form S-3 and Form SF-3 and Safe Harbor Provision in Exchange Act Rules 13a-11 and 15d-11 27

C. Disclosure about Cybersecurity Incidents in Periodic Reports 32

1. Updates to Previously Filed Form 8-K Disclosure 32

2. Disclosure of Cybersecurity Incidents that Have Become Material in the Aggregate 33

D. Disclosure of a Registrant's Risk Management, Strategy and Governance Regarding Cybersecurity Risks 35

1. Risk Management and Strategy 35

2. Governance 38

3. Definitions 41

E. Disclosure Regarding the Board of Directors' Cybersecurity Expertise 44

F. Periodic Disclosure by Foreign Private Issuers 48

G. Structured Data Requirements 49

Is Your Cybersecurity Strategy Falling Victim to These 6 Common Pitfalls?

NIST research reveals misconceptions that can affect security professionals — and offers solutions.

Here's a pop quiz for cybersecurity pros: Does your security team consider your organization's employees to be your allies or your enemies? Do they think employees are the weakest link in the security chain? Let's put that last one more broadly and bluntly: Does your team assume users are clueless?

Your answers to those questions may vary, but a recent article by National Institute of Standards and Technology (NIST) computer scientist Julie Haney highlights a pervasive problem within the world of computer security: Many security specialists harbor misconceptions about lay users of information technology, and these misconceptions can increase an organization's risk of cybersecurity breaches. These issues include ineffective communications to lay users and inadequately incorporating user feedback on security system usability.

"Cybersecurity specialists are skilled, dedicated professionals who perform a tremendous service in protecting us from cyber threats," Haney said. "But despite having the noblest of intentions, their community's heavy dependence on technology to solve security problems can discourage them from adequately considering the human element, which plays a major role in effective, usable security."

The human element refers to the individual and social factors impacting users' security adoption, including their perceptions of security tools. A security tool or approach may be powerful in principle, but if users perceive it to be a hindrance and try to circumvent it, risk levels can increase.

A recent report estimated that 82% of 2021 breaches involved the human element, and in 2020, 53% of U.S. government cyber incidents resulted from employees violating acceptable usage policies or succumbing to email attacks.

Haney, who has a comparatively unusual combination of expertise in both cybersecurity and human-centered computing, wrote her new paper, "Users Are Not Stupid: Six Cyber Security Pitfalls Overturned," to help the security and user communities become allies in mitigating cyber risks.

"We need an attitude shift in cybersecurity," Haney said. "We're talking to users in a language they don't really understand, burdening them and

belittling them, but still expecting them to be stellar security practitioners. That approach doesn't set them up for success. Instead of seeing people as obstructionists, we need to empower them and recognize them as partners in cybersecurity."

The paper details six pitfalls that threaten security professionals (also available in this handout), together with potential solutions:

1. **Assuming users are clueless.** Though people do make mistakes, belittling users can result in an unhealthy "us vs. them" relationship between users and cybersecurity professionals. Research on nonexperts reveals that users are simply overwhelmed, often suffering from security fatigue. A potential solution involves building positive relationships with users while empowering them to be active, capable partners in cybersecurity.

2. **Not tailoring communications to the audience.** Security pros often use technical jargon that reduces audience engagement, and they may fail to tailor lessons in ways that appeal to what users care about in their daily lives. Several strategies can help, from focusing on plain-language messages to presenting information in multiple formats to enlisting the help of an organization's public affairs office.

3. **Unintentionally creating insider threats due to poor usability.** Users who are already pushed to their limit by time pressures or other distractions can unwittingly become threats themselves, as they become prone to poor decision making. (As one example, complex password policies can inspire poor decisions, such as using the same password across multiple accounts.)

Offloading the user's security burden can help, such as by exploring whether more mail filtering can be done by the server so that fewer phishing emails get through. Also, when piloting new security solutions, testing the approach first with a small group of users can reveal potential confusion that can be corrected before a wider rollout.

4. **Having too much security.** "Too much" implies that a security solution may be too rigid or restrictive for the specific job context. While always using the most secure tools available sounds wise in principle, some users can find the resulting complexity stifling for daily work, leading them to violate security policies more frequently. Instead of a "one size fits all" stance, performing a risk assessment using a risk management framework can help determine what level of cybersecurity best fits a given environment.

5. **Depending on punitive measures or negative messaging to get users to comply.** Negative reinforcement is common within

organizations today: Examples include disabling user accounts if security training is not completed and publicly shaming individuals who cause cybersecurity incidents.

Whether or not these measures work in the short term, they breed resentment toward security in the long term. Instead, offering positive incentives for employees who respond to threats appropriately can improve attitudes toward security, as can taking a collaborative approach with struggling users.

6. **Not considering user-centered measures of effectiveness.** As employees often find security training to be a boring, check-the-box activity, how much of it are they actually retaining? Without direct user feedback and concrete indicators of behavior, organizations can struggle to answer that question.

It helps to think of concrete metrics as symptom identifiers — such as help desk calls that reveal users' pain points and incidents like phishing clicks that can show where users need more support.

After identifying the symptoms, security teams can use surveys, focus groups or other direct interactions with users to determine the root cause of problems, as well as improve their solutions.

Haney stressed that not all security professionals have these misconceptions; there are certainly security teams and organizations making positive progress in recognizing and addressing the human element of security. However, these misconceptions remain prevalent within the community.

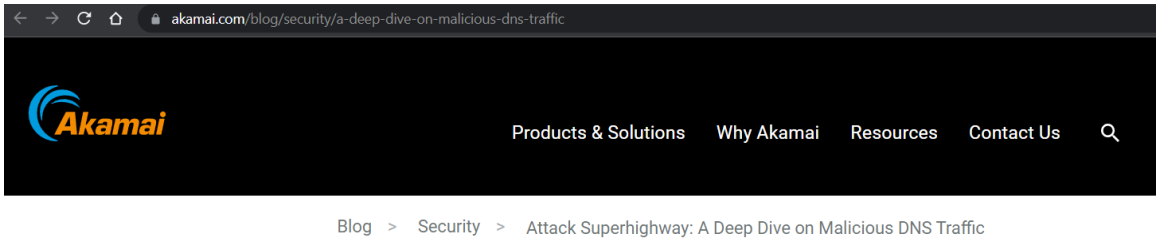
Haney said that though the issue with neglecting the human element has been well known for years — her paper cites evidence from industry surveys, government publications and usable security research publications, as well as her research group's original work — there is a gap between research findings and practice.

"There has been a lot of research into this issue, but the research is not getting into the hands of people who can do something about it. They don't know it exists," she said. "Working at NIST, where we have a connection to all sorts of IT experts, I saw the possibility of bridging that gap. I hope it gets into their hands."

To read more: https://www.nist.gov/news-events/news/2023/03/your-cybersecurity-strategy-falling-victim-these-6-common-pitfalls

DNS data shows one in ten organisations have malware traffic on their networks

An investigation by Akamai has shown that between 10% and 16% of organisations had Domain Name System (DNS) traffic originating on their network towards command-and-control (C2) servers associated with known botnets and various other malware threats.



The report also showed that over 9% of devices that generated C2 traffic, did so to domain names associated with known ransomware threats. Of these, REvil and LockBit were the most common ones.

The NCSC has produced guidance on the selection and deployment of protective DNS and there is also the Protective DNS for public sector

organisations at: https://www.ncsc.gov.uk/guidance/protective-dns-for-private-sector

To read more: https://www.ncsc.gov.uk/report/threat-report-24th-march-2023

https://www.akamai.com/blog/security/a-deep-dive-on-malicious-dns-traffic

Preventing the Improper Use of CHIPS Act Funding

The CHIPS Act (the Act) established an incentives program to reestablish and sustain U.S. leadership across the semiconductor supply chain.

To ensure that funding provided through this program does not directly or indirectly benefit foreign countries of concern, the Act includes certain limitations on funding recipients, such as prohibiting engagement in certain significant transactions involving the material expansion of semiconductor manufacturing capacity in foreign countries of concern and prohibiting certain joint research or technology licensing efforts with foreign entities of concern.

The Department of Commerce (Department) is issuing, and requesting public comments on, a proposed rule to set forth terms related to these limitations and procedures for funding recipients to notify the Secretary of Commerce (Secretary) of any planned significant transactions that may be prohibited.

Background

Semiconductors are essential components of electronic devices that enable telecommunications and grid infrastructure, run critical business and government information technology and operational technology systems, and are necessary to a vast array of products, from automobiles to fighter jets. Recognizing the criticality of supply chain security and resilience for semiconductors and related products, the President signed the Executive Order on America's Supply Chains shortly after taking office in February 24, 2021.

This Executive order, among other things, directed several Departments to undertake assessments of critical supply chains; several of the resulting reports address microelectronics and related subcomponent supply chains.

The resulting June 2021 White House Report on Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth highlighted the insufficient domestic manufacturing capacity for semiconductors.

The White House Report noted that the United States lacks advanced semiconductor manufacturing capabilities and is dependent on geographically concentrated and in some cases potentially unreliable sources of supply.

It recommended dedicated funding to advance semiconductor manufacturing, and research and development to support critical manufacturing, industrial, and defense applications.

In August 2022, the Congress passed the CHIPS Act of 2022, which amended Title XCIX of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, also known as the Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act.

Together, these statutory provisions (collectively, the CHIPS Act or Act), establish a semiconductor incentives program (CHIPS Incentives Program) that will provide funding, including via grants, cooperative agreements, loans, loan guarantees, and other transactions, to support investments in the construction, expansion, and modernization of facilities in the United States for the fabrication, assembly, testing, advanced packaging, production, or research and development of semiconductors, materials used to manufacture semiconductors, or semiconductor manufacturing equipment.

The CHIPS Incentives Program aims to strengthen the security and resilience of the semiconductor supply chain by mitigating gaps and vulnerabilities. It aims to ensure a supply of secure semiconductors essential for national security and to support critical manufacturing industries. It also aims to strengthen the resilience and leadership of the United States in semiconductor technology, which is vital to national security and future economic competitiveness of the United States.

The CHIPS Incentives Program is administered by the CHIPS Program Office (CPO) within the National Institute of Standards and Technology (NIST) of the United States Department of Commerce. CPO is separately issuing Notices of Funding Opportunity (NOFO) that lay out the procedures by which interested organizations may apply for CHIPS Incentives Program funds, and criteria under which applications will be evaluated.

To protect national security and the resiliency of supply chains, CHIPS Incentives Program funds may not be provided to a foreign entity of concern, such as an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a country that is engaged in conduct that is detrimental to the national security of the United States. This proposed rule incudes a detailed explanation of what is meant by foreign entities of concern, as well as a definition of “owned by, controlled by, or subject to the jurisdiction or direction of.”

In further support of U.S. national security interests, CHIPS Incentives Program recipients (funding recipients) are required by the Act to enter into an agreement (required agreement) with the Department restricting

engagement by the funding recipient or its affiliates in any significant transaction involving the material expansion of semiconductor manufacturing capacity in foreign countries of concern.

In recognition that some potential applicants for CHIPS Incentives may have existing facilities in foreign countries of concern, and to minimize potential supply chain disruptions, the Act includes exceptions for certain transactions involving older (legacy) semiconductor manufacturing in a foreign country of concern.

A funding recipient must notify the Secretary of any planned significant transactions of the funding recipient or its affiliates involving the material expansion of semiconductor manufacturing capacity in a foreign country of concern, including in cases where it believes the transaction is allowed under the exceptions in 15 U.S.C. 4652(a)(6)(C)(ii).

Terms related to this notification requirement are defined in Subpart A of this rule. The Secretary will provide direct notice to the funding recipient that a review of a transaction is being conducted and, later, that the Secretary has reached an initial determination regarding whether the transaction is prohibited. Funding recipients may submit additional information or request that the initial determination be reconsidered, after which the Secretary will provide a final determination.

In making determinations, the Secretary will consult with the Director of National Intelligence and the Secretary of Defense.

The Secretary will initiate review of transactions by funding recipients through self-reported notifications; the Secretary also may initiate a review of non-notified transactions, including based on information provided by other government agencies or information from other sources.

Failure by a funding recipient (or its affiliate) to comply with this restriction on semiconductor manufacturing capacity expansion in foreign countries of concern may result in recovery of the full amount of Federal financial assistance provided to the funding recipient (referred to in the Act as the “Expansion Clawback.”)

The Act also prohibits funding recipients from knowingly engaging in any joint research or technology licensing effort with a foreign entity of concern that relates to a technology or product that raises national security concerns as determined by the Secretary and communicated to the funding recipient before engaging in such joint research or technology licensing. A funding recipient's required agreement will include a commitment that the funding recipient and its affiliates will not conduct prohibited joint research or technology licensing. Failure to comply with this restriction

may also result in recovery of the full amount of Federal assistance (referred to in the Act as the “Technology Clawback.”)

To read more:
https://www.federalregister.gov/documents/2023/03/23/2023-05869/preventing-the-improper-use-of-chips-act-funding

#StopRansomware: LockBit 3.0

Note: this joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail ransomware variants and ransomware threat actors.

These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware.

Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing & Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate known LockBit 3.0 ransomware IOCs and TTPs identified through FBI investigations as recently as March 2023.

The LockBit 3.0 ransomware operations function as a Ransomware-as-a-Service (RaaS) model and is a continuation of previous versions of the ransomware, LockBit 2.0, and LockBit.

Since January 2020, LockBit has functioned as an affiliate-based ransomware variant; affiliates deploying the LockBit RaaS use many varying TTPs and attack a wide range of businesses and critical infrastructure organizations, which can make effective computer network defense and mitigation challenging.

The FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

Capabilities

LockBit 3.0, also known as “LockBit Black,” is more modular and evasive than its previous versions and shares similarities with Blackmatter and Blackcat ransomware.

LockBit 3.0 is configured upon compilation with many different options that determine the behavior of the ransomware.

Upon the actual execution of the ransomware within a victim environment, various arguments can be supplied to further modify the behavior of the ransomware.

For example, LockBit 3.0 accepts additional arguments for specific operations in lateral movement and rebooting into Safe Mode (see LockBit Command Line parameters under Indicators of Compromise).

If a LockBit affiliate does not have access to passwordless LockBit 3.0 ransomware, then a password argument is mandatory during the execution of the ransomware. LockBit 3.0 affiliates failing to enter the correct password will be unable to execute the ransomware.

The password is a cryptographic key which decodes the LockBit 3.0 executable. By protecting the code in such a manner, LockBit 3.0 hinders malware detection and analysis with the code being unexecutable and unreadable in its encrypted form.

Signature-based detections may fail to detect the LockBit 3.0 executable as the executable's encrypted potion will vary based on the cryptographic key used for encryption while also generating a unique hash.

When provided the correct password, LockBit 3.0 will decrypt the main component, continue to decrypt or decompress its code, and execute the ransomware. LockBit 3.0 will only infect machines that do not have language settings matching a defined exclusion list.

However, whether a system language is checked at runtime is determined by a configuration flag originally set at compilation time. Languages on the exclusion list include, but are not limited to, Romanian (Moldova), Arabic (Syria), and Tatar (Russia). If a language from the exclusion list is detected, LockBit 3.0 will stop execution without infecting the system.

To read more: https://www.cisa.gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf

Stopping cybercriminals from abusing security tools

Microsoft

Microsoft's Digital Crimes Unit (DCU), cybersecurity software company Fortra™ and Health Information Sharing and Analysis Center (Health-ISAC) are taking technical and legal action to disrupt cracked, legacy copies of Cobalt Strike and abused Microsoft software, which have been used by cybercriminals to distribute malware, including ransomware.

This is a change in the way DCU has worked in the past – the scope is greater, and the operation is more complex. Instead of disrupting the command and control of a malware family, this time, we are working with Fortra to remove illegal, legacy copies of Cobalt Strike so they can no longer be used by cybercriminals.

We will need to be persistent as we work to take down the cracked, legacy copies of Cobalt Strike hosted around the world. This is an important action by Fortra to protect the legitimate use of its security tools.

Microsoft is similarly committed to the legitimate use of its products and services. We also believe that Fortra choosing to partner with us for this action is recognition of DCU's work fighting cybercrime over the last decade. Together, we are committed to going after the cybercriminal's illegal distribution methods.

Cobalt Strike is a legitimate and popular post-exploitation tool used for adversary simulation provided by Fortra. Sometimes, older versions of the software have been abused and altered by criminals.

These illegal copies are referred to as "cracked" and have been used to launch destructive attacks, such as those against the Government of Costa Rica and the Irish Health Service Executive. Microsoft software development kits and APIs are abused as part of the coding of the malware as well as the criminal malware distribution infrastructure to target and mislead victims.

The ransomware families associated with or deployed by cracked copies of Cobalt Strike have been linked to more than 68 ransomware attacks impacting healthcare organizations in more than 19 countries around the world.

These attacks have cost hospital systems millions of dollars in recovery and repair costs, plus interruptions to critical patient care services including delayed diagnostic, imaging and laboratory results, canceled medical procedures and delays in delivery of chemotherapy treatments, just to name a few.

Disruption components and strategy

On March 31, 2023, the U.S. District Court for the Eastern District of New York issued a court order allowing Microsoft, Fortra, and Health-ISAC to disrupt the malicious infrastructure used by criminals to facilitate their attacks.

Doing so enables us to notify relevant internet service providers (ISPs) and computer emergency readiness teams (CERTs) who assist in taking the infrastructure offline, effectively severing the connection between criminal operators and infected victim computers.

Fortra and Microsoft's investigation efforts included detection, analysis, telemetry, and reverse engineering, with additional data and insights to strengthen our legal case from a global network of partners, including Health-ISAC, the Fortra Cyber Intelligence Team, and Microsoft Threat Intelligence team data and insights. Our action focuses solely on disrupting cracked, legacy copies of Cobalt Strike and compromised Microsoft software.

Microsoft is also expanding a legal method used successfully to disrupt malware and nation state operations to target the abuse of security tools used by a broad spectrum of cybercriminals.

Disrupting cracked legacy copies of Cobalt Strike will significantly hinder the monetization of these illegal copies and slow their use in cyberattacks, forcing criminals to re-evaluate and change their tactics. Today's action also includes copyright claims against the malicious use of Microsoft and Fortra's software code which are altered and abused for harm.

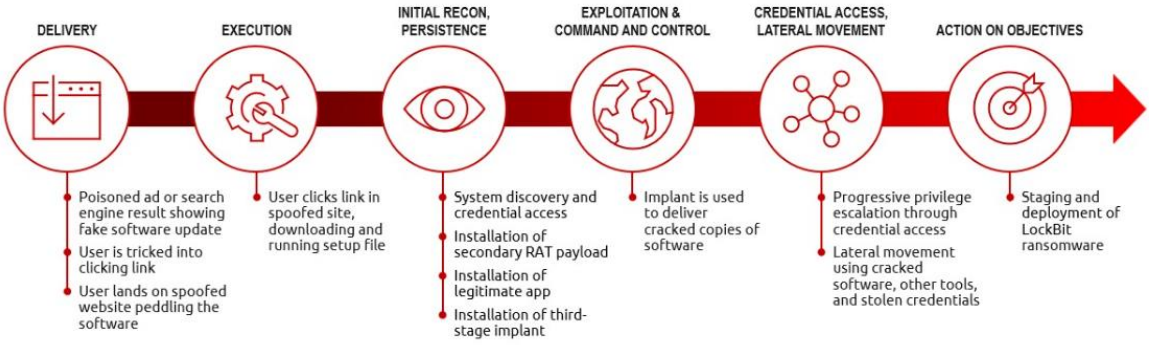
Abuse by cybercriminals

Fortra has taken considerable steps to prevent the misuse of its software, including stringent customer vetting practices. However, criminals are known to steal older versions of security software, including Cobalt Strike, creating cracked copies to gain backdoor access to machines and deploy malware.

We have observed ransomware operators using cracked copies of Cobalt Strike and abused Microsoft software to deploy Conti, LockBit, and other ransomware as part of the ransomware as a service business model.

Threat actors use cracked copies of software to speed up their ransomware deployment on compromised networks. The below diagram shows an attack flow, highlighting contributing factors, including spear phishing and malicious spam emails to gain initial access, as well as the abuse of code stolen from companies like Microsoft and Fortra.

While the exact identities of those conducting the criminal operations are currently unknown, we have detected malicious infrastructure across the globe, including in China, the United States and Russia. In addition to financially motivated cybercriminals, we have observed threat actors acting in the interests of foreign governments, including from Russia, China, Vietnam and Iran, using cracked copies.



To read more: https://blogs.microsoft.com/on-the-issues/2023/04/06/stopping-cybercriminals-from-abusing-security-tools/

New OpcJacker Malware Distributed via Fake VPN Malvertising

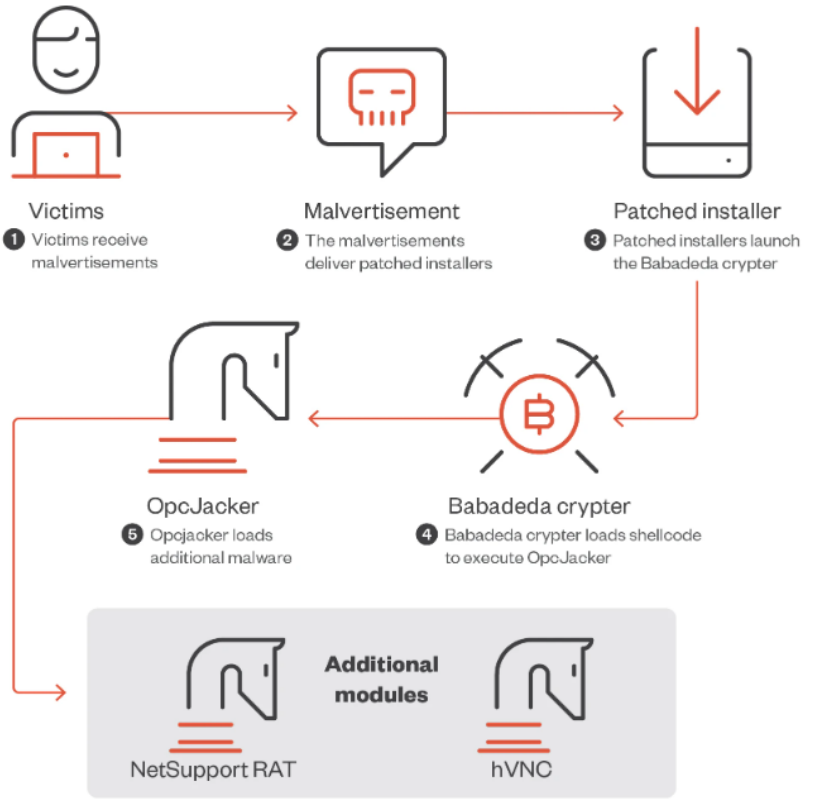
We discovered a new malware, which we named “OpcJacker” (due to its opcode configuration design and its cryptocurrency hijacking ability), that has been distributed in the wild since the second half of 2022.

OpcJacker is an interesting piece of malware, since its configuration file uses a custom file format to define the stealer’s behavior.

Specifically, the format resembles custom virtual machine code, where numeric hexadecimal identifiers present in the configuration file make the stealer run desired functions.

The purpose of using such a design is likely to make understanding and analyzing the malware’s code flow more difficult for researchers.

OpcJacker’s main functions include keylogging, taking screenshots, stealing sensitive data from browsers, loading additional modules, and replacing cryptocurrency addresses in the clipboard for hijacking purposes.



To read more: https://www.trendmicro.com/en_us/research/23/c/new-opcjacker-malware-distributed-via-fake-vpn-malvertising.html

Considerations for a Central Bank Digital Currency

Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at the Georgetown University McDonough School of Business Psaros Center for Financial Markets and Policy, Washington DC

It is a pleasure to be with you today to discuss the evolving money and payments landscape in the United States, which is a topic of primary importance to the Federal Reserve.

Technological innovation has changed this landscape in recent years, as we have seen the emergence of new financial services entrants offering payments services, new platforms designed to increase the speed of payments, clearing, and settlement, and new forms of digital money.

Over the past several years, and as a direct result of these developments, we have seen a significant increase in attention on central bank digital currencies (CBDCs) from central banks around the world in addition to a great deal of international and domestic engagement on CBDC.

A number of central banks have taken steps to begin exploring the potential uses of a CBDC in their home countries.

A very small number have adopted a CBDC for their local jurisdictions. And of course, discussions of the purpose, design, and potential risks of a U.S. CBDC, and technical research about key design elements, continue here in the United States.

While the Federal Reserve plays an important role in these ongoing discussions and technical research, the Fed would not implement a U.S. CBDC without the approval of Congress.

In broad terms, a CBDC is simply a new form of digital liability of a central bank. Because it is issued by a central bank, CBDC is typically thought of as being denominated in the currency of that central bank.

One could imagine a digital U.S. dollar, a digital euro, or a digital pound. Beyond this baseline definition though, “what is a CBDC” defies a simple definition.

A CBDC built on distributed ledger technology offers a wide range of design and potential use options, as well as potential risks. This variability

complicates any discussion of a CBDC simply because we may not be talking about the same thing.

There are two threshold questions that a policymaker needs to ask before any decision to move forward with a CBDC.

First, what problem is the policymaker trying to solve, and is a CBDC a potential solution?

Second, what features and considerations—including unintended consequences—may a policymaker want to consider in deciding to design and adopt a CBDC?

While it would be impossible for me to provide a comprehensive analysis of every issue surrounding CBDC, my goal today is to offer a perspective on these two threshold questions and to conclude with some thoughts about the imperative for future research on CBDCs and the potential future of CBDCs in the United States.

To read more: https://www.bis.org/review/r230419c.pdf

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: https://www.sarbanes-oxley-association.com/How_to_become_member.htm

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: https://www.sarbanes-oxley-association.com/Reading_Room.htm

3. Training and Certification - You may visit: https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We tailor all programs to meet specific requirements.