NIST IR 8050

EXECUTIVE TECHNICAL WORKSHOP ON IMPROVING CYBERSECURITY AND CONSUMER PRIVACY

Summary and Next Steps

Leah Kauffman
Nate Lesser
National Cybersecurity Center of Excellence
Information Technology Lab

Brian Abe
The MITRE Corporation
McLean, VA

DRAFT
April 2, 2015
consumer-nccoe@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NISTIR 8050

EXECUTIVE TECHNICAL WORKSHOP ON IMPROVING CYBERSECURITY AND CONSUMER PRIVACY

Summary and Next Steps

Leah Kauffman
Nate Lesser
National Cybersecurity Center of Excellence
Information Technology Laboratory

Brian Abe
The MITRE Corporation
McLean, VA

April 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

ABSTRACT

Cybersecurity incidents have grown swiftly from conceivable to realized risks that regularly threaten national and economic security of the United States. These risks threaten the financial security of companies and the public, weaken consumer confidence, erode individual privacy protections, and damage the brand value and reputation of businesses. On February 12, 2015 the National Institute of Standards and Technology (NIST) and Stanford University hosted an executive technical workshop, held in coordination with the White House Summit on Cybersecurity and Consumer Protection, to discuss how to increase the use of advanced cybersecurity and privacy technologies in consumer-facing organizations. This document details the discussion and ideas presented at the workshop and serves as a platform to receive broader feedback on the relevance of projects and suggestions discussed at that event.

KEYWORDS

adaptive security; advanced detection; authentication; consumer protection; consumer-facing; cybersecurity; cybersecurity framework for critical infrastructure; cybersecurity standards; data integrity; decentralized systems; incident response; multi-factor authentication; privacy

DISCLAIMER

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: consumer-nccoe@nist.gov

Public comment period: *April 2, 2015 – May 17, 2015*

ACKNOWLEDGEMENTS

The authors would like to thank Dr. Amy Zegart and Dr. Herbert Lin of Stanford University, Ms. Kiersten Todt of Liberty Group Ventures, as well as the workshop participants who provided valuable input to this report.

INTRODUCTION

On February 12, 2015 the National Institute of Standards and Technology (NIST) and Stanford University hosted a workshop with chief technology officers, chief information officers, and security executives in consumer-facing organizations to discuss how to increase the use of advanced cybersecurity and privacy technologies throughout their sectors.

This document is a summary of the workshop, which was held in coordination with the White House Summit on Cybersecurity and Consumer Protection. The National Cybersecurity Center of Excellence (NCCoE) will initiate projects—described in the "Next Steps" section—informed by the workshop. NIST is seeking broader feedback on the relevance of these projects and suggestions about additional steps that can be taken to foster improvements across these diverse organizations.

NIST would like feedback on the topics and ideas contained in this document. Respondents should include the name of the person or organization filing the comment, although anonymous comments will be accepted. All comments received are a part of the public record and will generally be posted to http://nccoe.nist.gov/consumer without change. Comments should be submitted at http://nccoe.nist.gov/consumer or by emailing them to consumer-nccoe@nist.gov. All personal identifying information (for example, name and address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information.

NIST is planning another workshop in the summer of 2015 to follow up on many of these same issues. For updates on future workshops and the most up-to-date status of the projects resulting from these workshops, visit http://nccoe.nist.gov/consumer.

SUMMARY

A wide variety of consumer-facing organizations were represented at the workshop, from banking and consumer products companies, to technology and health care providers, with differences in geography, scale and available resources. Despite the range of businesses represented, with different infrastructures and risk profiles, several key points emerged as potential focus areas for future work. At the highest level, given their interactions with consumers, participants quickly came to consensus that security, privacy, and usability concerns are paramount as they consider protections for corporate and customer information and assets.

Participants discussed the need for organizations to protect both consumer and corporate data. While consumers might consider businesses to be responsible for the customer data they hold, the workshop participants saw this as a shared responsibility. In addition to the security programs they put in place, organizations can help strengthen cybersecurity protections for their customers through education, training, transparent and clear privacy policies, and cybersecurity measures that are easier for consumers to use.

Much of the focus of the day also looked at how to get cutting-edge cybersecurity technology into the hands of those in industry that deploy it. There were discussions around how software and application developers should be seen as consumers as well, and that often the demand for additional features and better performance inhibits developers from incorporating more sophisticated security features. The participants concluded that developer tools, therefore, should make it easier to include security in software, without compromising performance. Automated security that reduces the need for human operators (e.g. tools that are able to dial up and down protection mechanisms based on a changing threat landscape) was another common theme.

On the topic of implementation, workshop participants agreed that cybersecurity products and services must be easier for security technologists to use. While a myriad of tools and technologies are available today, there are serious challenges to adoption in consumer-facing organizations.

Specifically, workshop participants articulated challenges in implementing a variety of technologies, including:

- authentication and multi-factor authentication
- advanced detection
- recovery tools
- adaptive security in response to a changing threat environment
- data integrity, not just data confidentiality
- third-party access to key corporate systems
- decentralized systems
- network traffic analysis

Finally, in addition to the issues above, workshop participants invited the entire cybersecurity community—people from government, industry, and academia—to collaborate to address the larger issues of security usability, consumer training, regulatory harmonization, third-party agreements and assessments, and transparency and clarity regarding privacy. Participants expressed a commitment to continue to work together on these issues and suggested that NIST could act as a convener for specific technical topics.

KEY POINTS

Workshop participants discussed in detail a variety of technical topics and challenges, described below.

Increase Education and Training

Further education and training for five broad populations was highlighted.

For consumers, the flexibility of technology and ease of use has trumped security historically. Consumers might see additional security controls as an annoyance. In general,

for this population, there are challenges in understanding the threat and steps individuals can take to protect their data.

For businesses, employees, not technologies, tend to be the weakest link in a business's security chain. Participants stated that security breaches, due to lost credentials, happen more often than breaches caused by malware, with employees falling prey to increasingly sophisticated phishing attempts. In addition, business owners and managers may not full understand the need to implement cybersecurity capabilities.

For developers, common programming mistakes and the reuse of code found online help to propagate unsecure applications. Additionally, participants stated that software release dates are often driven by the need for increased functional requirements making it difficult for developers to adequately account for security as part of the software development life cycle.

For cybersecurity professionals, high demand in the marketplace creates significant career mobility. While beneficial in elevating cybersecurity concerns, this also demonstrates the need for more well trained cybersecurity professionals. Consistency across training mechanisms (certifications, degree programs, vocational training) is necessary to ensure this workforce remains up-to-date on the latest cybersecurity challenges and solutions as it grows to meet demand.

Protect Privacy

Consumers interact with retailers and providers in a variety of ways enabled and enhanced by networked technologies: joining shopper rewards program, paying bills from a digital wallet, registering with online sellers to automate and track purchases, using mobile applications for purchases on the go, completing health records and managing bank accounts online. These capabilities have changed user experiences while allowing retailers and providers to collect customer, client, and patient data with a greater level of veracity, but they also pose privacy concerns to people who entrust businesses with their personal information, payment card data, and purchase patterns. This trust can only be maintained if the personal data of customers, clients, and patients is properly secured. Participants said that the loss of corporate reputation among the people they serve is more damaging and concerning than non-compliance with regulation and even potentially the loss of corporate data. The stakes for organizations are extremely high in this arena and further enhance the need for corporations to prioritize the implementation of technology to increase these protections.

Make Security Easier

Organizations of all sizes, but particularly smaller organizations with proportionally-sized resources, need technology that simplifies security instead of relying on individual expertise. Technical solutions must be easily integrated and user friendly. Those that are difficult to integrate, configure, and maintain essentially create their own barrier to entry because they become expensive and require a higher level of subject matter expertise that

is not attainable for every business. Additionally, technical solutions must consider how they integrate with users and business processes. Simplifying these integrations will reduce cost and other barriers to implementation. Workshop participants also expressed a need for tiered security measures, so that different kinds of employees with different levels of access can be easily granted different levels of security.

Detect and Act Early

Businesses must have the ability to detect attacks – which are seen as inevitable – as soon as possible. New technologies are needed to improve detection. This could include assistance with sorting through large amounts of network and system data, reduction in false positive alerts, and identification of useful intelligence about an attack. Once detected, it is important to eliminate the threat, and quickly evaluate the extent of any compromised.

Independent of detection, proactive measures are also an important component of quick-reaction solutions. Businesses must be able to reduce their attack surface and therefore reduce the complexity, variability, and cost associated with security. Building agility into the security solution will allow organizations to shift controls to new threat vectors independent of an attack taking place.

Make Authentication Stronger and More Useable

Workshop participants agree that passwords alone no longer provide sufficient protection for the assets they are meant to safeguard. The security infrastructure, therefore, must be transitioned to rely on stronger authentication and authorization mechanisms, including two-factor authentication. There are, however, challenges associated with this approach. Any given organization is likely to have a different tolerance for balancing risk, security, and usability for its employees and customers. For example, executives might mandate two-factor authentication for employees, but hesitate to do so with customers due to the risk of losing those customers to competitors.

While new technologies and approaches are emerging and consumer adoption is increasing, consumer-facing organizations worry about backlash from moving to stronger authentication technologies. If a security measure negatively impacts the user experience, the consumer may choose a competitor's easier-to-use service. This makes it risky for a company to force its consumers away from passwords. Companies that allow consumers to opt for two-factor authentication find that they usually don't, perhaps due to limited awareness of the security shortcomings associated with password authentication. Effective education is need to help ease consumers' adoption of stronger authentication mechanisms.

Address New Payment Technologies

Even as new credit card payment methods become mainstream, consumers still have a traditional notion of the payment experience: they hand their card to a salesperson and it is returned with a receipt needing a signature. Workshop participants speculated about how

new payment methods such as credit cards with chip-and-pin technology work amidst those expectations, and suggested that more consumer education is required to increase use of these more secure methods. Nevertheless, they agreed that traditional credit cards will not go away quickly, and new risks will continue to emerge. Therefore, it remains vital to identify mechanisms for securing existing magnetic swipe-based transactions.

To compound the issue surrounding payment in general, there are several distinct, yet connected, components of the systems that must be considered. First, the payment type itself can vary. Consumer-facing organizations contend with touchless payment options, new cards with imbedded chips, and traditional credit cards. Then, there is diversity among point-of-sale systems themselves. They can range from devices that plug into a smart phone to standalone systems that do not do real-time processing, to integrated systems that feed directly into an organization's network. The ecosystem that supports the transmission of the data from the point-of-sale device to the financial institution introduces an additional set of complexities as well. Each component and variation of the system comes with its own security challenges and potentially the need for distinct technology solutions to provide enhanced protection of consumer data.

Increase Focus on Data Integrity

As organizations assess their risks, they often focus on what can be stolen and used for profit, like intellectual property or customer records. Workshop participants stated that organizations also need to be concerned with data integrity. For example, instead of only being stolen in a breach, data can also be altered to cause financial harm, compromise safety of customers or workers, and disrupt a supply chain. Workshop participants indicated that data integrity is often overlooked when focusing on confidentiality and availability.

Account for Decentralized Environments

Decentralized workforces increase the complexity of an organization's security profile in two ways. First, a company must deal with varying laws and regulations; second, a decentralized IT infrastructure makes it more difficult to ensure that updates and patches are distributed and implemented. Companies that have branches run by franchisees find it difficult to standardize security profiles because the national brand doesn't necessarily have proper oversight mechanisms.

Secure Third-Party Access

For the purposes of conducting day-to-day business, organizations commonly allow third parties (customers, vendors, contractors, service providers, and others) to access their networks, systems, and data. This access needs to be evaluated, controlled, and accounted for in organizations' risk management plans. Ascertaining how these relationships affect an organization's risk posture is both non-trivial and critical. Participants discussed the need for guidance on how to better structure these relationships and implement protections around critical assets.

Make Attacks More Costly and Demonstrate that Security Pays

Most perpetrators of cybersecurity attacks do not experience consequences, and attacks can be launched with little investment in personnel, equipment, or software. Technology is key to making attacks harder to perpetrate, more costly to attackers, and easier to investigate. To avoid indiscriminately spending limited resources, business must understand what information is valuable so they can focus on what needs the most protection. Additional steps like data encryption and intelligent data separation can make it harder for attackers to gain valuable data.

Traditionally, when digital assets like customer and employee records were a byproduct of traditional business models, security was a function of the IT department. Now that those records can be businesses' most valuable assets, safeguarding them must be thought of as a key business driver. Information technology security executives must think of security in terms of business value. To get the attention of chief executives, chief information, technology, and information security officers need to use metrics that resonate with their business leaders, communicating clear outcomes that can be accomplished through investments in security.

Balance Between Regulation and Security

While largely out of scope for this workshop, participants noted that when regulatory compliance and security are in conflict, companies often prioritize regulatory compliance. This issue is compounded in sectors where organizations are subject to regulations that differ by jurisdiction or function.

Apply the NIST Cybersecurity Framework to Consumer-Facing Organizations

The NIST Framework for Improving Critical Infrastructure Cybersecurity was discussed several times during the workshop as a tool to help consumer-facing organizations to understand, communicate, and manage cybersecurity risk in the context of their enterprise mission and business objectives. Participants expressed interest in understanding how NIST and other cybersecurity standards, practices, and reference implementations relate to the Framework, and how those resources can help consumer-facing organizations achieve their cybersecurity priorities.

Existing Resources

NIST is not the only organization addressing cybersecurity in consumer-facing organizations. Many of the ideas expressed at the workshop dovetail with existing programs in government, industry working groups and trade associations, academia, and public-private partnerships. The Appendix to this document lists NIST programs dedicated to enhancing cybersecurity.

NEXT STEPS

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) collaborates with technology vendors to demonstrate standards-based example solutions to cybersecurity challenges using commercially available products. Below is a list of potential projects under consideration that directly addresses some of the issues raised during the technical workshop. Feedback will help determine prioritization – with a goal of beginning with projects that would be most beneficial to consumers and consumer-facing organizations.

We are seeking comments on the potential projects described below. Are these the most valuable projects? Are they scoped correctly? How should these efforts be prioritized? Are there higher priority projects on which we should focus?

Data Integrity

The NCCoE is considering a project that provides and verifies data integrity. For these purposes, a violation of integrity can be viewed as any unauthorized change in data, malicious or accidental, that is not immediately detected and remedied. The project might explore database integrity, file integrity, system integrity, and the integrity of backups. Technologies to examine might include auto-journaling file systems, cryptographic file checksums, detailed auditing, virtual machine snapshots, and versioning software.

This project might explore specific questions, including:

- What was altered during a breach?
- What was the impact of the data alteration? This examination needs to include traditional IT, mobile, cloud, and mainframe systems.
- From which backup version should an organization restore?
- After discovering and removing malicious code operating in an organization's environment, from which backup version should the organization restore data, applications, and services?

In addition to ensuring that the backup is of a known "good" image, this project should examine questions of how to ascertain that vulnerabilities, weakness, and malware are not reintroduced during the restoration.

What existing technologies enable organizations to maintain the integrity of systems, applications, files, databases, and backups?

Relevant Cybersecurity Framework Functions and Categories: PR.DS, PR.IP, PR.PT, DE.AE, RS.RP, RS.AN, RS.MI, RC.RP, RC.IM.

Developer Tools

Software systems have become increasingly complex, even while developers try to shorten development cycles. Complexity breeds flaws, which can be exploited to breach system security. As network security improves, attackers are targeting applications directly. To help address this growing software complexity problem, the NCCoE is considering a project to demonstrate the capabilities of software developer tools and environments that increase software assurance. This project might include static analysis, component architecture, dynamic analysis and other runtime analysis tools, and live vulnerability scanning and penetration analysis techniques.

This project might explore specific questions, including:

- What tools, development environments, and techniques enable secure code development?
- What tools can be put in the development environment to provide meaningful real-time feedback to improve developer knowledge on secure coding techniques, as well as integration-level feedback to catch vulnerabilities?
- Which existing and/or emerging languages provide inherent security benefits and what is needed to increase the use of these languages?
- What tools can be implemented to analyze external libraries and services as well as externally developed code components?

Relevant Cybersecurity Framework Functions and Categories: ID.AM, ID.BE, ID.RA, ID.RM, PR.AC, PR.AT, PR.DS, PR.IP, PR.MA, PR.AT PR.PT.

What existing technologies enable automated code reviews including static analysis, runtime analysis including dynamic analysis, live vulnerability scanning, and penetration analysis?

Automated Information Sharing and Incident Response

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the nation. Barriers to participation in information sharing initiatives include cost, liability concerns, lack of standards, lack of a mutual taxonomy, and technology gaps related to automated anonymization, ingestion, filtering, and incident response. To help reduce these barriers, the NCCoE is considering a project that demonstrates technical tools and methods for the automated sharing and use of cybersecurity information.

This project might address a number of specific questions, including:

- How can trusted and unknown partners securely share sensitive data, such as the actual attack vector detected or vulnerability identified?
- Can data be anonymized to address sensitivity, privacy concerns, and legally protected information?
- Can protection tools and measures be readily updated through the exchange of standards-based threat indicators?
- What technologies can automate the response to (and recovery from) a security breach once detected.
- What current technology blends the need for human-in-the-loop responses to new and sophisticated cyber-attacks with tools that learn from those responses?

Relevant Cybersecurity Framework Functions and Categories: ID.RA, ID.RM, PR.DS, PR.MA, PR.PT, DE.AE, DE.CM, DE.DP, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM.

What existing technologies enable and automate sharing of sensitive information, anonymization, machine learning, and incident response resolution?

Point of Sale/Payment Cards

To address concerns surrounding the use and implementation of point-of-sale systems and payment options such as traditional swipe cards, chip and pin cards, and touchless payments, the NCCoE is considering a project to demonstrate security mechanisms that can better protect information related to a consumer transaction.

This project might address a number of specific scenarios, including:

Technologies that can help secure different payment options

- How can an organization deploy technology to better secure consumer information for customers who use touchless payment options?
- How can the organization enhance the security around the wireless connection portion of the transaction?
- What other attack vectors might circumvent the security features of new payment technologies?

Enhanced security for point-of-sale systems

- Are new point-of-sale devices providing enhanced protection to avoid the loss of consumer data from traditional cards?
- Are new point-of-sale devices providing enhanced protection to avoid the loss of consumer data from new payment options?

- If not, what are other technologies that can be implemented to provide enhanced security for customers who continue to use traditional credit cards?

Relevant Cybersecurity Framework Functions and Categories: ID.AM, PR.AC, PR.DS, PR.MA, PR.PT, DE.AE

What existing technologies enable increased security for different payment options and point-of-sale devices?

External Entity Access

Allowing an external entity to access internal IT infrastructure, resources, and data creates a multitude of security issues. Whether the external entity is a different organization or a different operating unit within the same organization, mechanisms are needed to protect critical business and organizational functions. To address these concerns, the NCCoE is considering a project to explore technologies that can be integrated to create secure connections between and among entities, as well as allow for the monitoring of data access and movement (inbound and outbound) as a result of these connections.

This project might explore specific questions, including:

- When connecting directly with external entities, what technologies can be employed to provide logical separation of data and ensure that the outside organization has access only to the resources necessary to conduct business?
- How can those technologies be configured to reduce or eliminate performance degradation of an organization's network, but still be secure?
- How can an organization monitor what is coming in through (and going out of the connection) to an outside entity? Can these technologies detect structured and unstructured data such as social security and credit card numbers or geolocation data passed through the connection?
- If the data shared with the outside entity is encrypted, what tools exist to still ensure that it contains only the appropriate information before leaving the security boundary?
- What can we do to provide protection for an organization's information that is outside its boundary?

Relevant Cybersecurity Framework Functions and Categories: PR.AC, PR.DS, PR.MA, PR.PT, DE.AE, DE.CM, DE.DP, RS.CO, RS.AN, RS.MI, RC.RP, RC.CO

What existing technologies can assess connections to external entities, monitor activity and the type of data transmitted, and can prevent access to off-limits resources?

COMMENTS

Feedback

NIST would like feedback on the topics and ideas contained in this document. Respondents should include the name of the person or organization filing the comment, although anonymous comments will be accepted. All comments received are a part of the public record and will generally be posted to http://nccoe.nist.gov/consumer without change. Comments should be submitted at http://nccoe.nist.gov/consumer or by emailing them to consumer-nccoe@nist.gov. All personal identifying information (for example, name and address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information.

NIST is planning another workshop in the summer of 2015 to follow up on many of these same issues. For updates on future workshops and the most up-to-date status of the projects resulting from these workshops, visit http://nccoe.nist.gov/consumer.

Join the Community

To develop a project, the NCCoE forms a community of interest made up of companies who are facing similar challenges. The community will help to ensure that any NCCoE work addresses the most pressing concerns of the community, and that the supporting architectures created accurately depict representative architectures from the community. Once a technical description of the problem is finalized, including a map of the necessary security characteristics to applicable standards and best practices, the NCCoE works with technology providers to bring products into a laboratory environment where they are joined together to create a potential solution. The NCCoE then publishes a practice guide to assist companies in adopting technologies with similar characteristics.

You can join the community formed around issues in your sector at any time. You'll get news about projects underway, requests to contribute comments, and alerts about newly-launched projects. Visit http://nccoe.nist.gov to explore our work and sign up for alerts from NCCoE.

APPENDIX: NIST RESOURCES

The NIST mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Computer Security Division

Conducts research and develops standard, guidelines, tests, and metrics for protecting non-national security federal information and communications infrastructure.
http://csrc.nist.gov/

Framework for Improving Critical Infrastructure Cybersecurity

Voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure to better manage and reduce cybersecurity risk, and foster cybersecurity risk management communications among internal and external organizational stakeholders.
http://www.nist.gov/cyberframework/

National Cybersecurity Center of Excellence

Develops example solutions that show how standards and best practices can be implemented in the real world. http://nccoe.nist.gov/ and http://nccoe.nist.gov/projects

National Initiative for Cybersecurity Education

Promotes development of a cybersecurity workforce. http://csrc.nist.gov/nice/

National Strategy for Trusted Identities in Cyberspace

Dedicated to more secure alternatives to passwords. NSTIC seeks to improve the privacy, security, and convenience of online transactions. http://www.nist.gov/nstic/

NIST Privacy Engineering Initiative

Developing a risk management approach for privacy within the federal government to facilitate better identification of privacy risk in information systems and support the development and implementation of more effective technical standards to mitigate privacy risk. http://csrc.nist.gov/projects/privacy_engineering/