IV.D. Cybersecurity & Risk Management

Key Recommendations

REC IV.D.1. Evaluate blockchain appropriateness based on the specific use case, considering financial and operational risk.

REC IV.D.2. To establish a new baseline of security and adequately trained workforce for this emerging technology, the State of California should encourage training for (and potential certification and licensing of) application developers who develop or supply blockchain platforms to the State of California.

REC IV.D.3. The State of California should create policies and standards to govern the use and control of blockchain utilizing industry expertise and other worldwide standards.

REC IV.D.4. Convene Blockchain Advisory Groups across relevant State Agencies composed of experts from academia and industry.

Introduction

As the fifth largest economy in the world, the State of California has an extraordinary influence on almost every aspect of commerce. The home of Silicon Valley, it leads the world on technology, including matters of data security and privacy. California was the first jurisdiction in the world to pass a law in 2002 mandating the disclosure of a data breach affecting Californians and was the first state in the U.S. to pass a privacy law in 2018, protecting the personal information of Californians. Any legislation on blockchain will have an effect on the California economy and beyond.

California's data breach disclosure law provides an extensive record of all publicly disclosed breaches since 2004. While this chronology does not offer guidance on how to prevent such breaches, it does provide a record of the types of problems government and private sector companies have failed to prevent.

In light of this, the State must carefully consider the risks and vulnerabilities of blockchain, and design controls to ensure that all users of the technology have mechanisms to appeal blockchain transactions in which the State is a participant until they are deemed secure enough to replace current practices. To the extent it is commercially reasonable to do so, operators of applications serving the private sector should be encouraged to have similar appeal mechanisms.

DETAILED RECOMMENDATIONS:

1. Application-specific evaluation of risks and mitigations. As with any new technology, blockchain's benefits and risks must be evaluated on a case-by-case basis until a body of knowledge establishes the most efficient and secure designs. Every class of application will present different priorities that may require trade-offs. The appropriate blockchain architectures should be used for different application contexts to manage financial and operational risk.

For example, while a home and an automobile are both assets typically purchased by consumers and registered with the State of California, given the different ecosystems these asset classes operate in, two separate blockchain-based systems to track these assets may be warranted. The same analogy applies to humans who participate in different ecosystems: healthcare, education, finance, government, employment, commerce, etc. Each ecosystem may deserve its own blockchain to support agency transactions within that ecosystem.

An important challenge will be striking the right balance between: (i) having sufficient diversity to limit the risk of a single large-scale security event; and (ii) keeping the total number of blockchains the State participates in manageable from a security perspective. The latter is an important consideration in an environment in which the pool of qualified personnel to provide security oversight, audit, and similar functions is limited.

The desire for privacy is not inherently contradicted by the immutability of blockchains. The State should consider that neither a blanket privacy law nor a rush to implement blockchain is an optimal answer. Government regulation of some aspects of blockchain development may address security concerns. While regulation does not guarantee the elimination of security breaches, the absence of regulation may create an environment for continued systemic breaches, which may exacerbate losses to consumers. An important consideration here is that any such regulation be introduced in a way that is *technology-neutral*, i.e., does not disadvantage blockchain technology relative to legacy technologies and thereby delay the introduction of this promising new technology. So, for example, if new security regulations are enacted they should, to the extent feasible, apply equal to traditional database technologies and not only to blockchain.

Transparency, e.g., precipitating public disclosures of key information, is an alternative to traditional regulation that regulators have used to encourage desirable behaviours related to some aspects of the Internet industry. Where transparency of information serves a public good, government leaders must make considered decisions to find the right balance.

2. Encourage training and potential certification of blockchain developers. The State of CA should create training policies and standards to govern the use and control of blockchain utilizing industry expertise and other worldwide standards. The State of California should encourage certifying the workforce of blockchain developers through working with industry and academic partners to develop institution-based curricula or professional development programs. The State's educational systems should convene a panel of application development experts from academia and industry to define an appropriate curriculum and explore certification.

3. Create policies and standards in accordance with industry-wide practice. To enable the State to make objective risk-management decisions with respect to blockchain application security, the State should be guided by best practices and guidance emerging from internationally recognized standards bodies.

The following may be considered for adoption:

Disruptive Defenses. Below is a summary of six best practices for any modern application operating within complex networked systems. The State is encouraged to evaluate potential blockchain applications with these in mind.

> **A. Eliminate *weak authentication technology***: One possible solution is the use of public-key cryptography. Looking to the longer term, technology suppliers should be encouraged to incorporate *crypto-agility* into their offerings, so that it will be possible to modernize the underlying cryptography as/when required. For example, NIST and its contemporaries are aware of the potential threat to public-key cryptography from future quantum computers. Accordingly, NIST has been conducting a program to standardize "post-quantum safe" cryptographic algorithms. Crypto-agile systems would reduce the cost and time required to transition to these new standards and would also enable the rapid mitigation of threats to conventional cryptography as/when they emerge.
>
> **B. Ensure the *provenance* of a transaction before it enters the blockchain**: Transactions should be digitally signed before they are submitted to the blockchain. Ideally, the *provenance* of transaction data originating in the physical world would be traceable, through a chain of signatures, all the way back to the point where the information was obtained from a human user or physical sensor. Realistically, this will not always be practical since, in many cases, the data entering blockchains will be sourced from existing legacy applications that lack such provenance records. This re-positioning of legacy applications as *blockchain frontends* will be essential to the rapid and smooth adoption of the technology.

C. Preserve the confidentiality of sensitive information within and outside the blockchain: The California Consumer Privacy Act (CCPA) requires protection, as do many laws around the world. Encryption is the industry standard for preserving the confidentiality of sensitive information. In general, even encrypted sensitive information should not be placed on widely accessible blockchains. Since encryption protection has a limited lifetime (typically a few decades) efforts should also be made to avoid placing long-lived sensitive information (such as healthcare records) on less accessible blockchains that lack strong access controls equivalent to those used with highly restricted databases.

Note that this does not preclude recoding a *digital thumbprint* of sensitive information on a blockchain provided the thumbprint cannot be used to reveal the sensitive information itself. Such a record could be used to verify the authenticity of sensitive *off-chain* information that is stored in a separately secured and less accessible system.

D. Provide transparency regarding the integrity of transaction data originating outside the blockchain: While a digitally signed transaction provides assurances about the *provenance* of the transaction, it cannot guarantee the integrity of the data itself. Commercially reasonable and technology-neutral efforts should be taken to validate and preserve the accuracy of the data when importing, updating or reversing records on the blockchain.

E. Cryptographic Algorithm Implementations and Key Management
The implementation of cryptography algorithms is complex and most crypto vulnerabilities arise from errors in the implementation rather than in the underlying algorithms themselves. Application developers unaccustomed to working with cryptography also underestimate the intricacies of key-management (the discipline of managing the life-cycle of cryptographic keys).

Blockchain applications using cryptographic keys for encryption and signing should consider using field-proven software packages and/or certified cryptographic hardware solutions to implement the underlying algorithms and/or to secure cryptographic keys, in adherence to NIST guidelines and in keeping with best practices of the industry.

An additional consideration related to hardware-based key management arises when personal keys are managed by members of the public. For various reasons, some individuals may not be able to prevent the physical object that stores their signing key (e.g., a USB-like key fob) from being lost or stolen, and they may not have ready access to the facilities, processes

and/or credentials that would restore their timely access to systems that provide them critical services.

F. Work with cloud computing providers, if appropriate, to ensure operational security. Cloud computing presents many opportunities for alternative deployment strategies for IT systems, as well as challenges for traditional notions of data security. For example, if moving data and computing from "on-premises" applications to the cloud, ensure that appropriate cryptographic controls are available and in place for blockchain applications.

4. Convene Blockchain Advisory Groups representing security experts from academia and industry to advise California agencies considering blockchain implementations. Given the paradigm shift that blockchain-based systems present for current systems, California agencies should establish Blockchain Advisory Groups representing the following categories of stakeholders:

- Business leaders, independent legal and privacy advisers, experts from industry and academia proficient in systems, application and cryptographic security
- Government representatives of existing systems-of-record (where public records are involved)
- Experienced regulators from other sectors such as construction, finance, utilities, etc.
- Representatives of the public who will be affected by the blockchain-based system

The Advisory Groups could establish a public online forum and invite security and cryptography experts from academia and industry to review security designs for blockchain applications and provide their feedback through a formal process of Request for Comments or other procedure.

CONSIDERATIONS AND OPPORTUNITIES FOR BLOCKCHAIN APPLICATION

Blockchain is a young technology. As such, practitioners have not yet identified best practices that can be applied to projects across the board. However, given that blockchain technology intersects fields of databases, network protocols and security, many relevant resources and research are available. Without a detailed understanding of each business application, its data model and the impact of business transactions on networks, it is difficult to make generalized recommendations in these areas.

While it has always been possible to share business transactions securely among interested parties within an ecosystem, blockchain technology may simplify

many aspects of this process, reduces the friction typically encountered in distributed database designs, and, because of the redundancy in the system, increases permanence and transparency.

On blockchain systems government data will remain permanently available for the public record. While this data-sharing must be subject to privacy regulations, it would be the equivalent of a permanent "freedom of information act" record available on the internet. It offers potential benefits to preserving democratic norms and holding the government accountable to its constituents.

While blockchain has its benefits, it does not eliminate all problems:

- If multiple companies and government agencies must collaborate on transactions to complete business processes, they must agree on transaction protocols and the rules that regulate those transactions. This process can be simple or burdensome depending on the use-case.
- Implementers must handle physical technology problems independent of the blockchain: hardware failures, network outages, security vulnerabilities, and the like. Multiple copies of the blockchain make data always available, which is also true of traditional databases. However, these costs must be taken into account when designing blockchain applications.
- Given the newness of this technology, there is a tendency to equate all blockchain implementations with "Bitcoin" blockchain. However, blockchain applications may be implemented in a variety of ways. State agencies should seek a thorough understanding of the use-case and the technical ramifications of the implementation.

Addressing vulnerabilities. The vast majority of data-breaches are caused by failures to protect data from known vulnerabilities; very few attacks are caused by "zero-day vulnerabilities," i.e., vulnerabilities that were never known until the attack and its methods were discovered.

Most vulnerabilities in any application can be addressed with stronger defenses. These defenses are not unproven new technologies but are based on current industry standards that raise application security to much higher levels.

While the use of these defenses cannot unequivocally prevent an application from being compromised (since not all threats can be mitigated, or the cost of mitigating all threats will make it prohibitively expensive to implement the application), a security compromise is more likely if one or more of these defenses are <u>not</u> incorporated.

California's data breach disclosure law of 2002 was bold for its time. However, it did not go far enough to have prevented the 11,000 publicly disclosed

breaches that followed: it did not mandate that the company or government agency publish a standardized forensic report documenting the breach and the mechanics of how it occurred.

When a data breach occurs today, most cybersecurity professionals without access to the evidence must deduce (at best) or guess (at worst) how it occurred and what might have prevented it. The industry that creates technology products and universities that train new generations of technology professionals have limited ability to prevent similar future breaches.

The field would benefit from regularly published blockchain Data Breach Forensic Reports, so that academia and the technology industry may learn from them and improve their designs and technology implementations. The cognizant State entity responsible for administering the data breach disclosure law should take steps to encourage and, if necessary, require the disclosure of Forensic Reports for all significant data breaches covered by the law, including those in blockchain platforms.

Adopt an experimental period for permissionless blockchain applications**.** The speculative nature of crypto-currencies and the dramatic events surrounding public blockchains, for example the collapse of Mt. Gox and the "hard fork" of the Ethereum blockchain, suggests that the State of California might consider defining an *experimental* period of perhaps 5-7 years, when implementations of blockchain-based *systems of record* are restricted to only private and/or permissioned blockchains, under the State's authority, for use-cases that reflect public data. This does not imply that the State may not implement blockchain-based applications; merely that in the early phases of adoption, the State avoid sole reliance on public, permissionless blockchains.

Initial experiments with permissionless blockchains might, for example, involve their use as secondary sources for validation of information in the Registry of Births, Deaths and Marriages, or the registration of Business Entities, where information is public by law. During such experimental periods the relevant State agencies would ensure that, in the event of a conflict, existing systems-of-record will be the primary authority. This will enable the State to enter the field cautiously and learn from its experience before taking bolder steps.